PERSONAL COMPUTER COMMUNICATIONS CLIENT (VOICE / VIDEO / COLLABORATION)

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

11 June 2008

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO or any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

1 INTRODUCTION 6

1.1 Scope and Applicability 6
1.1.1 Relationship to Other STIGs 8
1.1.2 Relationship to CNSSI 5000 and 5001 RE: On-Hook/Idle Audio Security 9
1.2 Authority 10
1.3 Writing Conventions 11
1.4 Vulnerability Severity Code Definitions 11
1.5 DISA Information Assurance Vulnerability Management (IAVM) 12
1.6 STIG Distribution 13
1.7 Document Revisions 13

2 VULNERABILITIES AND IA REQUIREMENTS 13

2.1 General Vulnerability Discussion and Background 13
2.2 Reliance on Platform (i.e., PC) OS Security – ECSC-1 18
2.3 Assured Service and Command and Control (C2) Communications 20
2.3.1 PC Based Communications Assured Service 22
2.4 User Operation of the Communications Application and Accessories 24
2.4.1 Information In View of a Camera 25
2.4.2 Audio Pickup and Broadcast 26
2.4.3 Visual Compromise of Session Displays 27
2.4.4 PC Data and Presentation Sharing 27
2.4.5 Audio and Video Capture When Not Communicating 28
2.4.6 Use of Soft-Phone Accessories 29
2.5 User Awareness and Operational Training, User Agreements, and User guides 31
2.5.1 Acceptable Use Policy – User Agreement 31
2.5.2 User Training and User's guides 32
2.6 Use Case Implementations and Protecting Critical Voice Communications 33
2.6.1 Strategic LAN Use Case 34
2.6.1.1 Unified Communications Applications in the Strategic LAN 35
2.6.1.2 Soft-Phones as Primary Voice Instruments in the Strategic LAN 36
2.6.1.3 Limited Numbers of Soft-Phones in the Strategic LAN 38
2.6.1.4 Voice/VTC Infrastructure Protection RE: PC Communications Applications 40
2.6.1.5 PC Soft-Phones and CTI Systems 42
2.6.2 Tactical PC Soft-Phone Use Case 43
2.6.3 PED/PDA Soft-Phone Use Case 45
2.6.4 Remote Access / Telework Use Case 45
2.7 Call Privacy and Confidentiality 47
2.8 Application Requirements 48
2.8.1 Certification, Accreditation, and Testing 48
2.8.1.1 DoDI 8100.3 Policy Compliance and DoD Approved Products List 49
2.8.2 Communications Application Origin 51
2.8.2.1 Freeware and Shareware 51
2.8.2.2 Reputable Source and Software Integrity 51

2.8.3 Vulnerability Management 53
2.8.4 Application IA Configuration Considerations 53
2.8.4.1 Administrative Privileges 53
2.8.4.2 Downloaded Configuration Files 53
2.8.4.3 Server or System Association 54
2.9 DoD Policy for Non-Official use of VoIP and IM - ECVI-1 and ECIM-1 55
2.10 DoD Ports, Protocols, and Services Management 58
2.10.1 PPS Registration 58

APPENDIX A - DEFINITIONS 60

A.1 Real-Time Communications 60
A.2 Near-real-time communications 60
A.3 Non-real-time or “best effort” communications 60
A.4 Real Time Services (RTS) 61
A.5 Voice Communications 61
A.6 Video Communications 61
A.7 Text Based Communications 61
A.8 Telephone or Phone 62
A.9 Speakerphone 62
A.10 Videophone 62
A.11 Soft-Phone 63
A.12 Computer Telephony Integration (CTI) 64
A.13 Voice over IP (VoIP) vs Circuit Switched Voice 64
A.14 Voice over IP and/or Video over IP - Acronym Confusion 65
A.15 Tele-Conferencing or Audio Conferencing 65
A.16 Video Tele-Conferencing (VTC) 65
A.17 Desktop VTC 66
A.18 Soft-VTC or Soft-VTU 66
A.19 Webcam 67
A.20 IP Television (IPTV) 67
A.21 IP Closed Circuit TV (IP CCTV) 67
A.22 Instant Messaging (IM) 68
A.23 Presence 68
A.24 “Web Based” Application 68
A.25 Web Conferencing 69
A.26 Collaboration 69
A.27 Collaboration Tool 69
A.28 Collaboration Application 70
A.29 Unified Messaging 70
A.30 Unified Communications 70
A.31 USB Phone 71
A.32 Analog Telephone Adapter (ATA) or Telephone Adaptor (TA) and USB ATA 71
A.33 Personal Phone Gateway (PPG) 72
A.34 Stick Phone / Flash Phone 72
A.35 Internet Telephony Service Provider 73
A.36 Strategic LAN 74
A.37 Tactical LAN 74

APPENDIX B - CNSSI 5000/5001 DISCUSSION 76
APPENDIX C - ACRONYMS 80
APPENDIX D - REFERENCES 84

LIST OF TABLES

Page

Table 1.2 – Vulnerability Severity Code Definitions 12
Table 2.1 – Network Availability Requirements 21
Table 2.2 – Methods of Expressing Availability 21

1 INTRODUCTION

A core mission for the Defense Information Systems Agency (DISA) Field Security Operations (FSO) Division is to provide guidance for securing all varieties of Department of Defense (DoD) communications networks and information systems. The processes and procedures outlined in this Security Technical Implementation Guide (STIG), when applied, will decrease the risk of unauthorized disclosure of sensitive or classified information. Information and communications security is one of the biggest concerns for our DoD customers (i.e., the warfighter).

The Personal Computer (PC) Communications Client STIG, addresses the Information Assurance (IA) issues surrounding the use and implementation of PC software applications that enable the PC to act as a client (i.e., an endpoint or end-instrument (EI)) for various interactive real-time and near real-time communications systems and services; many of which enable collaboration in one form or another. All of the communications clients addressed here can be considered collaboration tools. Also addressed are configuration, implementation, and architecture requirements for the platforms and networks that support the applications and communications. The guidance contained herein is applicable to all levels of information sensitivity and Information System (IS) classification.

Note: For the purpose of this document, PC will refer to any computer that is used by a person and acts as a host for a communications/collaboration client application. This will most typically be the user's primary administrative workstation but may also be a workstation that serves some other purpose. It is recommended that the reader familiarize themselves with the terms and definitions contained in Appendix A for a better understanding of the terms and concepts used in this document. These definitions also provide some insight to the roots and the complexity of today's PC based communications applications. Also included are definitions of various PC accessories or peripherals used with these applications.

1.1 Scope and Applicability

The primary focus of this STIG is PC applications and accessories that enable voice and video communications with IP based telephone and VTC systems, however, the STIG also addresses other forms of PC based communications/collaboration services and applications. Today, many of these same PC based telephone and VTC applications also provide other forms of near-real-time interactive and non-real-time data and text based communications. Communications services that were once based in separate applications are now merging into single all inclusive communications applications or suites of applications that can be quite complex. While there are a wide range of applications available that provide the same or similar services, they have been developed from different roots. This STIG addresses these additional applications, in part, due to their ability to also provide voice and video communications services requiring similar IA guidance. Additionally addressed are configuration, implementation, and architecture requirements for the PC platforms, their connection to a supporting network, and certain aspects of the network configuration in conjunction with other related STIGs. Server side issues and the overall communications/collaboration system architecture is not addressed.

The following is a list of the types of applications addressed and some of their features:

- **Soft-Phone Application**: Primarily enables the PC to act as a telephone endpoint to a VoIP telephone system or service. Can provide additional services such as video communication and click-to-dial.

- **Soft-VTC Application**: Primarily enables the PC to act as a Video Teleconferencing (VTC) endpoint associated with a hardware based VTC system typically found in conference rooms and executive offices while providing similar capabilities.

  Note: the VTC STIG addresses hardware based VTC systems and endpoints. The guidance in this STIG augments the guidance in the VTC STIG and parallels it in some areas where the vulnerabilities or possible compromises are similar.

- **Instant Messaging (IM) or Chat Application**: Primarily enables text based communications between two or more persons in near-real-time. Typically includes **Presence Services**. Can provide additional services such as voice and video chat; file transfer or sharing.

  Note: the Collaboration (or IM) STIG addresses IM servers and endpoint applications (clients). The guidance in this STIG augments the guidance in that STIG and parallels it in some areas where the vulnerabilities or possible compromises are similar.

- **Web Conferencing/Collaboration Application:** Primarily enables the PC to act as an endpoint in a multi-party conference (as chair/host or participant) using a web browser application; Provides some or all collaboration services found in VTC systems; Minimally provides the ability to share documents and presentations with other conference participants from a server or by sharing the PC screen or an application. May enable white boarding and collaborative markup and editing of documents. May provide a web based IM (text chat) and presence service. Can provide additional services such as voice/video communications. Often used with an external voice conferencing system.

- **Unified Communications (UC) Application**: Primarily intended to add capabilities to voice communications by integrating multiple communication methods and PC applications as described above into a single application. Different UC applications provide different capabilities but typically provide presence, IM, voice, video, and collaboration services. Feature sets within each communications type or method also vary from application to application. In some instances, a UC application's soft-phone functionality can serve as the primary voice instrument in a user's workspace. A UC application can also coordinate with, and enable additional features for, a hardware based telephone (VoIP or not) collocated in the user's workspace.

Note: Additional information on each of these applications can be found in Appendix A.

The intent of this STIG is to provide security and implementation considerations that will result in an acceptable level of risk for sensitive information (unclassified or classified) located in, on, or near the PC, the protection of the information being communicated, and the protection of the critical systems that enable and carry the communications. This breaks down as follows:

- "Information in/on the PC" is any and all data contained within the PC to include its memory, hard drive, or both. This includes information displayed on the display or "desktop" that is not part of the "the information being communicated". Such information is vulnerable to improper disclosure through the use of desktop, screen, or application sharing.
- "Information near the PC" is any aural (i.e., sound), or visual information that occurs or exists in the area where the PC is located. This includes conversations that might be picked up by a microphone, information that can be "seen" by a camera, or both. Such information is not part of the "The information being communicated" and is vulnerable to improper disclosure through the use of microphones and cameras.
- "The information being communicated" means the information being transmitted or received. Such information is vulnerable to improper disclosure to individuals that are not party to the communications session. This could be persons in, or near, a workspace where the communications session is occurring.
- "The critical systems that enable and carry the communications" are the networks, telephone systems, and VTC systems that the PC based applications, software, and tools become part of as a client/endpoint, or with which it communicates. The security and protection of such systems is or can be, reduced or the system made more vulnerable, due to the implementation of the PC based applications.

Note: For the purpose of this document the term "sensitive information" means information that is not classified (i.e., unclassified) but is worthy of protection from disclosure to individuals that do not have a need or right to be aware of, or to know, the information. Such information might be marked For Official Use Only (FOUO) or could be related to privacy, personnel records, procurement, strategic planning, designs, specifications of unclassified systems or networks, and so forth. It could be any information that if improperly disclosed could be detrimental to a person, program, organization, or could give an undue advantage to an individual or organization. Also for the purpose of this document the term "classified information" is any information that is related to or part of a program or other information that has been formally classified (confidential or above) under DoD or Federal guidelines.

1.1.1 Relationship to Other STIGs

Overall guidance for DoD voice and video communications is contained in several other STIGs as follows:

- Defense Switched Network (DSN) STIG (Unclassified Voice, Traditional and VoIP)
- Voice over Internet Protocol (VoIP) STIG (Unclassified and Classified VoIP)
- Defense RED Switched Network (DRSN) STIG (Classified Voice, Traditional and VoIP)
- Video-Teleconferencing (VTC) STIG (Hardware based VTC systems, dial-up or IP)

The guidance in this STIG augments the guidance contained in the STIGs listed above with the exception that this STIG replaces section 3.6 of the VoIP STIG v2r2, dated 21 April 2006, in its entirety including the requirements contained therein. Section 3.6 relates specifically to IP Soft-Phones. The other requirements are unchanged.

In addition, this STIG augments the guidance contained in the Collaboration, or Instant Messaging (IM) STIG which addresses IM and Web based collaboration tools. This augmentation addresses the voice and video communications capabilities in these applications as well as other information and presentation sharing capabilities.

The scope of this STIG is limited to the secure use and implementation of PC based real time near real time communications applications including their external accessories or peripherals. Implementation guidance includes requirements that affect the configuration of the network(s) to which the PC is attached. This additional guidance augments that contained in the VoIP STIG as well as the network related STIGs such as the Enclave, Network Infrastructure, and Secure Remote Computing STIGs.

This STIG also requires the implementation or use of other STIGs where applicable. The most notable of which is the Operating System (OS) and networking/remote access STIGs as they relate to the PC. In addition the server side of the various communications and collaboration applications discussed in this document are subject to all applicable STIGs for example, IM/Collaboration, OS, Web Server, Application Services, Database, and so forth.

1.1.2 Relationship to CNSSI 5000 and 5001 RE: On-Hook/Idle Audio Security

On-Hook/Idle Audio Security measures address vulnerabilities in the design of telephone instruments that give them the undesirable ability, while on-hook which is an idle or powered off state, to pick up and transmit over the wire conversations occurring in its general vicinity. A serious security liability occurs when a telephone possesses this vulnerability. It provides a point from which someone can monitor conversations in a workspace.

On-hook audio security is addressed by several standards published by the Committee on National Security Systems (CNSS) and the National Telecommunications Security Working Group (NTSWG), formerly known as the Telecommunications Security Group (TSG). These are TSG Standards 1 through 8, NTSWG Standard 2a, and CNSS Instructions (CNSSI) 5000 and 5001. Standard analog, computerized, and VoIP telephones and systems are addressed. The NTSWG plans to update and reissue the TSG and NTSWG Standards as CNSSIs.

Director of Central Intelligence Directive (DCID) No. 6/9, requires TSG Standards and Information Series compliance by Sensitive Compartmented Information Facilities (SCIFs) for the protection of sensitive information and unclassified telecommunications information processing systems and equipment; SCIF compliance shall now be fulfilled in accordance with the appropriate CNSSIs.

While this STIG addresses vulnerabilities and their mitigations that are similar to those addressed by the NTSWG guidance, this release does not address the policy and guidance contained in the NTSWG documents or in other policy documents that reference them.

Additional information on these standards and where they can be obtained can be found in Appendix B, along with a discussion regarding the extensibility of these requirements to other communications devices that possess microphonic capabilities such as VTC endpoints and PCs. Additionally discussed is the applicability of on-hook audio security to areas other than SCIFs where sensitive or classified conversations can occur.

Note: Best practice dictates the implementation of all communications systems with endpoints that are designed to meet on-hook audio security requirements, whether the environment is unclassified or classified. Doing so will limit or eliminate the ability for an endpoint to allow aural information to be improperly disclosed through a design flaw or its compromise.

Note: It is quite possible that the Director of Central Intelligence may determine that PCs and monitors that have embedded microphones are to be banned for used in a SCIF due to the possibility or likelihood that the device cannot meet on-hook audio security requirements. These requirements are rather stringent and currently (as of March 08) there are no VoIP telephones that meet them. PCs with attached microphones could also be banned, however, it is easier to control the potential compromise of these devices through disconnection or the use of positive mute/disconnect switches. Cameras, embedded or not, pose similar threats, even though their lens can be covered.

1.2 Authority

DoD Directive 8500.01E requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DoD Directive 8500.01E.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

Additionally, DoD Instruction 8100.3 which governs DoD Voice Networks, refers to the DoDD 8500.1 (IA policy) and DoDI 8500.2 (IA implementation), for IA requirements regarding system certification and accreditation. Some requirements in this document may be derived directly from the 8100.3 such as those regarding the DoD Unified Capabilities (UC) Approved Products List (APL) (UCAPL). For the purpose of this document, the use of APL refers to the DoD UCAPL. Additional information on the APL can be found at the following web site: http://www.disa.mil/gs/dsn/ops_connect.html.

1.3 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" indicates mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written.

For each italicized policy bullet, the text will be preceded by parentheses containing the STIG Identifier (STIGID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows: "(*G111: CAT II*)." If the item presently does not have a STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "*[N/A: CAT III]*"). Throughout the document accountability is directed toward the IAO to ensure a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. All reasonable attempts to meet this criterion will be made.

1.4 Vulnerability Severity Code Definitions

Severity Category Codes (CAT) are a measure of risk used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III. Each policy is evaluated based on the probability of a realized threat occurring and the expected loss associated with an attack exploiting the resulting vulnerability.

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall. PC communication client vulnerabilities that provide immediate access to the configuration settings of a PC, the communications client, immediate unauthorized access to communications session information/media, and immediate unauthorized, or improper disclosure of information located in the area of the PC based communications endpoint
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder. PC communication client vulnerabilities that provide a high potential of giving access to the configuration settings of a PC, the communications client, unauthorized access to communications session information/media, unauthorized, and improper disclosure of information located in the area of the PC based communications endpoint
Category III	Vulnerabilities that provide information that potentially could lead to compromise. PC communication client vulnerabilities that potentially could lead to compromise giving access to the configuration settings of a PC and/or the communications client, unauthorized access to communications session information/media, unauthorized and/or improper disclosure of information located in the area of the PC based communications endpoint

Table 1.2 – Vulnerability Severity Code Definitions

1.5 DISA Information Assurance Vulnerability Management (IAVM)

The DoD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DoD. The IAVM process provides notification of these vulnerabilities and alerts require that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site: https://www.jtfgno.mil or https://www.cert.mil. Access restrictions apply.

1.6 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the following NIPRNet web sites:

- DoD IA Portal on Defense Knowledge Online (DKO); https://www.dko.dod.mil or more specifically https://www.us.army.mil/suite/page/397960
- Information Assurance Support Environment (IASE) web site; http://iase.disa.mil or more specifically http://iase.disa.mil/stigs/index.html.

These sites contain the latest release of all STIGs, checklists, scripts, and other related security information.

Additionally, the IASE web site is the source for all applicable STIGs, checklists, and tools to be used by vendors that are preparing for, or are involved in, IA testing of their voice, video, VTC, and related products pursuant to DoD UCAPL listing.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DoD organizations before inclusion in this document.

2 VULNERABILITIES AND IA REQUIREMENTS

2.1 General Vulnerability Discussion and Background

As IP networking and computing technologies have developed over the years, they had not been designed to be inherently secure. Security and IA measures were an afterthought, developed to mitigate vulnerabilities in response to compromises. The approach has classically been make it work first, focus on features second, and then to “bolt on” security measures (and then only if needed due to a discovered flaw or vulnerability) instead of making it organic to the development process. This situation is improving, in that security and IA are being considered and in some cases addressed by vendors during development, particularly in the case of maturing products. However, the “bolt on” mindset is still active, particularly in the development of emerging technologies as in the case of PC based communications applications.

IP networks are subject to such threats as Denial of Service (DoS), address spoofing, sniffing, man in the middle attacks, and more. These threats affect the availability of the network as well as the confidentiality and integrity of the information conveyed by it. Additionally, by the inherent design of the network, just about anything attached to it is accessible through it thereby, making attached devices vulnerable to unauthorized access. Such access can permit compromise of the information contained therein and allow the device to be used for unauthorized purposes.

Unauthorized access is also an issue for the networking devices such as routers and switches. As technology advances, and we can do more and more with our computing devices and the networks we connect them to, the more vulnerabilities and avenues for attack there are. Attackers are continually developing new exploits and methods for compromising our systems. These can be based on the inherent nature of the network and devices or can be based on errors in programming or configuration.

We must protect against the threats and vulnerabilities inherent in, and those that are continually emerging against, our IP networks and attached computing devices. To do so, various physical and technological mitigations or protections are employed. Due to the fact that no single one of these is, or can be, fully effective against all threats in a networked environment, a layered defense strategy must be used. Such a defense strategy means employing many different mitigations and protections in many different places and at various layers in our overall network architecture. This is called Defense in Depth.

In contrast, traditional dial-up voice and video communications are not subject to the multitude of vulnerabilities inherent in today's IP based networks. The purpose-built nature of the switching equipment and the limitations of physical access to it, severely limits the ability to compromise the switching system as easily as an IP connected computing device. By the fact that each communications device (i.e., endpoint) connects to the switching device via a dedicated cable pair, compromise of the communications is made more difficult because physical access to the endpoint or cable pair serving it is required. Even though this technology is not fully secure, it is far less vulnerable to many threats than today's IP networks.

Additionally, the traditional voice communications systems and services as provided by both public and private wired telephone systems have classically been highly reliable and highly available while being viewed as relatively secure. As a result of this, these systems and services have become critical to mission success and life safety in our day to day private, business, and military lives. Conversely, the need to support mission critical and life safety communications has driven these traditional systems to become highly reliable. In order for IP based systems to replace the traditional voice communications systems and services, the same level of reliability, high availability, and security, is expected, and must be achieved in IP based systems. IP systems and services are therefore being driven to improve and excel in these areas. Unfortunately this is a huge, costly task due to the increased number of threats to and the nature of IP based systems and services.

Availability is one of the biggest concerns for mission critical and life safety communications. While the core of our IP networks can be made highly available and reliable, primarily through the use of redundancy, the edge of the network, that is the user device (i.e., the PC) and network connection to it is not so fortunate. A PC can be made highly available and reliable if it is dedicated to a specific task and protected from compromise. The function it provides can be made more available and reliable if it is provided with two network connections from different redundant network nodes. While this may be done for special situations, it is unrealistic for the general user's PC. This is primarily based on cost. Additionally, the more functions added to a PC, the more vulnerabilities and threat vectors it has, and the more unreliable and unstable it can become. All of this reduces the availability factor of the PC which can become a real issue for implementing reliable and highly available communications use cases on the PC. If the PC is compromised, availability is reduced further.

The trend in communications systems is to reduce the cost of communicating, and do more with the communications system. As such, VoIP was originally seen as a method of reducing the cost of long distance telephone service by using the Internet. While this is still the case today in the service provider arena, internal business communications systems are also migrating to VoIP technologies as a cost saving measure. This can be based on the fact that implementing a business VoIP system can eliminate the installation of the dedicated cable plant and a costly switching system required by a traditional phone system.

Another cost saving situation is that the equivalent of the traditional switching systems are now being built on general purpose computing platforms (e.g., servers), operating systems (e.g., Windows and Linux), and other applications (e.g., database and web server). Due to these factors, a business VoIP system is seen as a money saving communications system. Unfortunately, this is only the case if the installation is new and the network is designed to be capable of supporting highly available VoIP. It is much less cost effective if a system requires replacement or upgrade.

Another advantage of implementing VoIP is that IP networks and computing devices can enable more features and flexibility in our voice communications systems than is easily achievable with a traditional system. VTC systems have taken a similar path while UC promises to integrate all of our communications methods and provide ground breaking feature sets in a single environment across multiple devices. This merging of voice and video communications with IP based data communications at the network and device level is called convergence. It is a strong driving force for technological development today.

There is no doubt that the convergence of our voice and video communications with our data networks and working toward Everything over IP (EoIP) has advantages over separate systems primarily in the areas of cost, productivity, and efficiency. While the relative improvement in these areas varies from system to system, this convergence greatly reduces the security of our communications. This security reduction is because the voice and video infrastructure and the supported communications inherit the vulnerabilities of the IP based network and those of the general purpose platforms, operating systems, and applications that are used. The addition of these communications services and applications also provides additional vectors for the compromise of the network, the attached hosts, and the platforms supporting the communications. Additionally, the reliability of our communications is negatively affected since IP based networks are designed for best effort conveyance of packets and not real time communications. Network technologies such as Quality of Service (QoS) and priority forwarding must be applied to IP networks supporting voice and video communications to increase the reliability and the quality of the traditional systems. The Mean Opinion Score (MOS) of voice calls on properly engineered IP networks must achieve the same QoS/MOS scores as traditional Time Division Multiplexing (TDM) voice networks.

Note: MOS is a traditional call quality measurement that is the numerical measure of the perceived quality of a telephone connection reflected in a range of 1 (bad) to 5 (excellent), with a minimum goal of 4(good). (wikipedia.org, 2008).

Due to the reduced reliability and increased vulnerability, IP based voice communications systems must be protected to a level that generally exceeds that afforded to our IP based data communications networks and platforms. IP based voice communications systems must also be protected from threats presented by the data infrastructure and hosts in the event they become compromised.

Additionally, the implementation of voice and video communications on an IP network, due to the nature of the protocols used, presents additional vulnerabilities to the traditional enclave and data Local Area Network (LAN). The needs of these protocols works against the protections afforded the traditional data LAN/enclave. Boundary protection is degraded and the VoIP system provides additional vectors for compromising the LAN and its attached devices.

The VoIP STIG provides additional guidance over and above the Network Infrastructure STIG that is needed to protect the voice infrastructure on a LAN within an enclave and to protect the enclave from the vulnerabilities added by the VoIP service (primarily at the enclave boundary). The goal of this guidance is to ensure that the voice infrastructure and supported communications is protected from compromise as best possible and remains viable even when the data network is degraded by compromise or is under attack.

The guidance requires the segregation of voice and data traffic on the LAN via the use of Virtual LANs (VLANs), Access Control Lists (ACLs), and separate voice and data IP address space (generally called subnets). This separation utilizes the nature of VLANs and their ability to isolate workgroups and protect traffic on the LAN from access by other workgroups.

The use of VLANs also has a benefit resulting in improved performance for the traffic it supports and reducing the possibility of network congestion. This is a standard Layer 2 LAN design practice which creates a traffic "management zone" for the protected workgroup or LAN service. Using Layer 3 and higher devices such as routers and firewalls, traffic into and out of this management zone can be controlled with the use of ACLs based on VLAN number and IP subnet. Standard network design practice makes full use of VLANs.

Even though VLANs are not designed as a security measure, thus they are not considered a "security tool", their use can be seen as providing a derived security benefit and thereby as providing some measure of security. As such, this can be considered as a VoIP "zone of protection" on a converged LAN, or as NSA has referred to it, a "security zone". The use of the term "security zone" in relation to the added security benefit of VLANs engenders great controversy and spirited discussion. Therefore for the purpose of this document, we will use the term "protection zone" to infer that some protection is afforded the service while those protections are not true security as might be provided by traffic encryption.

A supporting argument for the use of VLANs in this manner is that the Network Infrastructure STIG provides for the use of a VLAN dedicated to in-band management traffic (if in-band management is used) to separate management traffic from user traffic. Properly implemented, this creates a protection zone for management traffic. It also requires that this traffic NOT utilize the default VLAN which is used for all traffic including LAN control plane traffic by default. Best practice would dictate that the default VLAN should be used only for network control plane traffic and that additional VLAN(s) be configured for user traffic. This can be viewed as providing separate protection zones for control plane traffic, management traffic, and user traffic. The user or data traffic VLAN can be viewed as a default or unprotected "data zone".

The VTC STIG also provides for a VTC protection zone or VTC VLAN (or VLANs) to be used to protect traffic from hardware based VTC endpoints.

Thus far our vulnerability discussion has focused on VoIP. This is primarily because voice is the most critical of the various real-time and near-real-time communications and/or collaboration services being converged with data services on our IP based networks. As noted previously, voice communications can be mission critical and failures can affect life safety. The importance of voice communications to mission is demonstrated by the development of priority capabilities in the circuit switched network for extra important calls. This is why our guidance focuses on the use of purpose built hardware based endpoints and their protection using a voice protection zone. VTC is the second most critical collaboration service to be protected by our guidance. This is because it has also become a mission critical communications media. It too uses purpose built hardware based endpoints worthy of protection using a VTC protection zone. VTC has generally been as reliable as voice communications because of the use of the circuit switched network with its priority capabilities.

As communications and collaboration services converge with data services on the IP network and the general purpose platforms connected to it, software based communications/collaboration endpoints running on a PC are more vulnerable and potentially less available than their hardware based counterparts. This is primarily due to threats and vulnerabilities in the platform and network supporting these applications that are not present in their hardware based counterparts.

Additionally, a communications/collaboration application that becomes compromised can become an avenue for the compromise of other such applications, the core equipment supporting them, and become a potential bridge between protection zones.

Caution must be exercised when relying on a software based PC communications tool/application. The mission benefits should outweigh the risks.

The remainder of this document will discuss these risks, other threats, and vulnerabilities while providing IA requirements for their mitigation.

2.2 Reliance on Platform (i.e., PC) OS Security – ECSC-1

A major IA issue surrounding the use of PC based communications applications is that they run on general purpose computing platforms using a general purpose operating system such as Windows. The security and availability of the communications application and the communications service it provides is dependent on the security and availability of the underlying platform and OS. The general purpose nature of the platform means other uses of the device may threaten the communications services.

PC platform vulnerabilities include such threats as viruses, Trojan horses, spyware, and other malicious code. To be more specific, the operating system and all applications including communications applications residing on the platform are modifiable and attackable by malicious code. Due to these threats a PC is not a reliable and secure platform by default. This is especially true if it is connected to the Internet/NIPRNet and stringent controls are not in place to prevent end-users from installing software, and accidentally becoming infected with malware or both. Once malicious software is on the PC it can do whatever it wants on the platform and the network. While the majority of these infections can create a denial-of-service situation on the platform and communications service or both, the greatest threat to communications applications operating on these platforms is the possibility that spyware or other malicious code could cause the confidentiality, integrity, and/or availability of the enclave's critical voice and video communications networks and sessions to be compromised.

There are various ways compromises could occur. Operation of the communications application is susceptible to communications interception / logging / recording on the platform. Some of this could be intentional as in the case of legitimate call/session recording software used for specific approved situations, but may also be malicious. Spyware could be written to record a conversation and send the file to a third party’s server for later replay. The communications application might be remotely controlled as when malicious code could activate the PC microphone and/or webcam to listen in on room conversations or view the activity in a room; or it could be used to place calls through it from other locations using some remote connection to the PC. Another possibility is the application might be modified to relay itself through a third party device creating a man-in-the-middle attack that could record the session or modify it and forward the modified message.

While all of these attacks could be possible on a dedicated hardware device, it is really the multitude of attack vectors on the PC that make it much riskier than a dedicated platform. As the dedicated platforms get more functions we may see this advantage disappear. The important thing is the end-user cannot install whatever software; does not surf the web with vulnerable web browsers; and is not opening email attachments on dedicated IP endpoints. The ability to lock down a single purpose device is much greater than for a multi-use device.

The vulnerabilities discussed here are essentially the same vulnerabilities that any application and its data are susceptible to while on the PC. One of the best and only ways to mitigate PC platform issues such as these is to configure the platform in accordance with the applicable OS STIG such as Windows, Unix. and MAC OSx, as well as the Desktop Application STIG to include its "Secure Remote Computing" requirements. Particular attention must be given to the installation and upkeep of the software that protects the platform as well as the security patching of the platform OS.

Furthermore, DoDI 8500.2 IA control ECSC-1 regarding "Enclave and Computing Environment/Security Configuration Compliance" states "For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied."

- *(RTS-PC 3120.00: CAT II) The IAO will ensure the PC or platform that hosts, or on which, a voice, video, UC, or collaboration application is installed is compliant with the STIGs that are applicable to the platform as follows:*
  - *Applicable Operating System STIG (e.g., Windows, Unix. and MAC OSx)*
  - *Desktop Application STIG*

  Specific emphasis is to be given to the following requirements in these STIGs:
  - *Anti-virus*
  - *Anti-Spyware*
  - *Personal Firewall*
  - *Host-Based Intrusion Detection System (HIDS)*
  - *Security patching of the platform OS (IAVM compliance)*
  - *Regular updates to the above measures and the operating system*

  Note: The JTF-GNO mandated DoD enterprise wide host based security tool is the DoD Host-Based Security System (HBSS). This tool is required on all windows PCs at this time. This tool is capable of providing many of the required services noted above as well as other services.

  Note: This requirement is not intended to determine the level of compliance with the applicable STIG. This is only a finding in the event the applicable STIG(s) have not been applied to the platform and/or the emphasized platform protections are not installed, appropriately configured, and active.

Note: The specifically emphasized items are already requirements in the applicable STIGs. They are mentioned here for reader awareness since communications applications rely heavily on these mitigations for their protection and security.

2.3 Assured Service and Command and Control (C2) Communications

"Assured service" refers to the set of capabilities used to ensure that mission critical communications are established and remain connected until completion. (From IETF Internet Draft - draft-pierce-sipping-assured-service-02.txt) Assured service capabilities primarily support military communications but have applicability in commercial networks and applications. Additionally, while the concept of assured service is normally applied to voice and possibly video, communications it can also be applied to mission critical data communications. The NCID T300 Version 2.0 characterizes this communication as "Precedence-based Assured Service (PBAS). This service implies that, in general, QoS requirements of a higher precedence class will be met at the expense of a lower precedence class if the network conditions do not allow meeting QoS requirements of all Service Classes."

The concept of assured service has traditionally been used in military telephone systems but is defined as Multi-Level Precedence and Preemption (MLPP) in both US and international traditional telecommunications standards. MLPP provides the capability on a telephone system to set precedence levels for a call and preempt calls of lower priority, if required, to assure the higher precedence call will be established and maintained. Implementing MLPP consists of a combination of trunk bandwidth/capacity management and the ability to pre-empt a busy station or call flow. Per the Real Time Services (RTS) Work Group (WG), the MLPP concept translates to assured service terms as bandwidth on demand for privileged users based on situational awareness of IP or traditional voice network conditions. This means that the system must have awareness of network availability, congestion, and endpoint status to assure a priority call can get through and be maintained even if it means pre-empting a lower priority call to obtain the required bandwidth or endpoint availability. This is similarly implemented in an IP Wide Area Network (WAN).

Establishing assured service capabilities in an IP network is not an easy task due to the inherent "best-effort" nature of such networks. Normally packets are forwarded as fast as possible providing there is capacity or available bandwidth in the path to be used. If this capacity is limited or the path is congested, packets have to wait or are discarded. Transmission errors can corrupt packets, also causing them to be unusable and possibly discarded. In some protocols such as UDP, lost packets are just that, lost. With others such as TCP, the packet can be re-transmitted. This behavior does not assure packet delivery.

Assured service in an IP network depends on several factors such as priority forwarding of specially marked packets, OoS, and the reliability and robustness (i.e., availability) of the network. Network availability is a factor of high bandwidth availability, redundancy, and diversity. As such, network availability must be extremely high to assure provided services will succeed. Next, to illustrate this, we reference the reliability specifications for an Assured Service LAN (ASLAN) supporting assured service supporting voice, video, and data.

Based upon the Unified Capabilities Requirements 2007 (UCR 2007) and draft UCR 2008, the current specifications for the reliability and availability of an ASLAN is four nines and a seven (99.997%) for C2 users; five nines (99.999%) for Special-C2 users; while C2-Routine and non-C2 users only need three nines (99.9%). Figure 2.1 and 2.2 are reproduced from the UCR to highlight this and what this means in terms of downtime per year.

LAN Type	Media Types Supported	Users Supported (see notes)	Requirements
ASLAN	Voice, video and data	Special C2	- 99.999% availability - 8 hr UPS - No single of point of failure for > 64 voice users
		C2	- 99.997% availability - 2 hr UPS - No single of point of failure for > 64 voice users
Non-ASLAN	Voice, video and data	C2(R) and non C2	- 99.9% availability - No UPS required - Single point of failure allowed for > 64 voice users
Legend: ASLAN - Assured Services LAN non-ASLAN - non-Assured Services LAN C2 - Command and Control C2(R) - C2 user (Originate Routine only calls) [2]			CJCSI - Chairman of the Joint Chiefs of Staff Instruction LAN - Local Area Network UPS - Uninterruptible Power System VoIP - Voice over Internet Protocol
Notes: 1. C2(R) users may originate Routine only calls but may terminate (receive) any precedence level. 2. C2 user definitions IAW CJCSI 6215.01C			

Table 2.1 – Network Availability Requirements

Number of 9's	Availability	Downtime per year
1	90.0%	36 days, 12 hrs
2	99.0%	87 hrs, 36 mins
3	99.9%	8 hrs, 46 mins
4	99.99%	52 mins, 33 secs
4 + a 7	99.997%	15 mins, 46 secs
5	99.999%	5 mins, 15 secs
6	99.9999%	31.5 secs
Legend: Hrs – Hours Mins – Minutes Secs – Seconds		

Table 2.2 – Methods of Expressing Availability

Assured service also relies on admission control in bandwidth constrained situations such as when session packets are traversing an access circuit into or out of an enclave LAN. With the exception of the access circuits or upstream connections to the backbone, DoD LANs and backbone networks are generally reliable and robust, possessing plenty of bandwidth in support of assured service. Assured service is hindered by the bandwidth constrained nature of most access circuits.

Note: Access circuits are the TDM or optical circuits between a backbone Service Delivery Node (SDN) and the LANs Customer Edge Router (CER) at the site's enclave boundary. Most access circuits have limited bandwidth when compared with internal LAN connections or a direct Ethernet connection to the SDN, thus creating the bandwidth constrained environment. Bandwidth is also constrained when using satellite links as do deployed tactical systems.

Another factor for providing assured service is the availability of the communicating endpoints. Dedicated hardware based communications endpoints (e.g., purpose built telephones and VTC devices) can be relied upon in most cases to be highly available to receive and make calls on short notice thus they are generally capable of supporting assured service. They are of course dependant upon power availability and the supporting network, but telephones are normally on and connected. VTC devices can be left on if inbound assured service calls are required but more often these are needed for a MCU hosted or other prescheduled conference.

To summarize, the success of Assured Service is dependant upon many factors, all of which must be properly orchestrated for it to work correctly. Much work is being done to establish capabilities in support of assured service voice communications. It is yet to be determined if this work will be successful in the near term. While it will most likely succeed in the robust strategic LAN and WAN environment, it may not in bandwidth constrained environments. However, as more services such as priority VTC, priority messaging, priority sensor telemetry, and so forth, vie for assured service capabilities, may not work well, because these services are most needed in the bandwidth constrained tactical environment.

2.3.1 PC Based Communications Assured Service

PC based communications applications rely on many different factors, but are dependant upon the platform on which they operate. A PC could be dedicated to a task, protected, and controlled such that it is highly available for mission critical applications and communications. However, a user's general purpose PC or other computing device may not be highly available for mission critical communications, particularly if it is not dedicated to that task. This because it supports many applications and functions while being connected to a network through which any number of threats can come. Mission critical applications and communications are also negatively affected if the PC is powered off, busy with another process, the communications application is not loaded or is not running properly, or if the PC is compromised and/or is having operational problems. While a fixed desktop or tower PC may be kept in a powered on and network connected state most of the time, a portable PC (laptop) is much more likely to be powered off and disconnected from the network. There is more chance that the PC and communications application won't work, or be available, when needed compared to a dedicated device such as purpose built hard phones or dedicated PCs.

Power for PCs is another consideration in our discussion of their support for assured services and mission critical systems, users, and locations. If there is no power in the user's workspace, the PC will not function unless a backup power supply is provided. Thus may be provided using a battery based Uninterruptible Power Supply (UPS) or a backup generator. Either solution is very costly when providing backup power to the workspace for the PC, particularly for large numbers of users. Provisions for light and other environmental factors may also be necessary adding to cost. On the other hand, power is much more easily provided to a hardware based phone from the wiring closet using the LAN cabling. A UPS or generator will still be needed but in a centralized location reducing cost.

Another factor is the robustness and reliability of the network to which the PC is connected. As noted above, DoD networks can and must be designed and controlled to provide the reliability and robustness needed to support assured service. This can work well for a dedicated communications endpoint but not necessarily for a PC communications application. This is because the PC will be connected to the portion of the LAN that carries normal data traffic by default. That is the portion of the LAN that can be compromised and degraded by various DoS attacks and other issues making it difficult for this portion of the LAN to provide assured service.

The VoIP STIG defines some of the LAN requirements for the support of assured service, most notably the separation of the voice assets and traffic on the LAN from the data assets and traffic while maintaining a converged LAN architecture. Various solutions may also be available that can allow a PC to mitigate or manage these issues. These will be discussed later in the LAN use case section of this STIG.

A remotely connected PC cannot be relied upon to support assured service if it is connected to a non-DoD network such as an Internet connected LAN or the internet itself. This is due to lack of DoD control over the network to which it is attached. While most non-DoD LANs and the Internet are relatively reliable and may be robust regarding bandwidth, there is no control over the conditions in, or the availability of, these networks, whether it is the LAN or WAN.

Based on the factors noted in the previous paragraphs, PCs cannot provide the reliability and availability required for assured service when compared to the reliability and availability specifications for a LAN supporting assured service. These factors make it difficult to consider a user's general purpose fixed or portable PC as being a stable platform for mission critical communications in an assured service sense even though we desire it to be so. All of these factors also affect non-assured service systems that provide life safety and emergency communications. In the future, PC and PC based communications application vendors may solve these problems and provide us with fully assured service capable PC based communications on a standard general purpose, general use platform at a reasonable cost.

These issues do not, however, preclude a PC based communications application from attempting to place and receive priority communications sessions. A C2 user may use this type of end instrument for the origination of, or reception of routine and non-routine calls at their discretion, as long as a purpose built instrument or other backup communications system/device is also available for use as a backup communications method when necessary. This however, may not be feasible in all situations such as when using a portable PC outside of the normal workspace.

- *(RTS-PC 1020.00: CAT II) The IAO will ensure C2 and Special-C2 users are made aware of the potential for unreliability and reduced availability of PC based communications for assured service / C2 communications in the various situations in which they might use their PC for this purpose. The IAO will additionally ensure C2 and Special-C2 users are made aware of the need for and availability of backup communications methods available/provided in these various situations.*
- *(RTS-PC 1030.00: CAT II) Within a C2 or Special-C2 user's normal workspace (e.g., office) or alternate workspace (e.g., quarters, alternate office), the IAO will ensure C2 and Special-C2 users are provided with an alternate assured service communications device/system (e.g., hardware based IP or traditional telephone endpoint) is provided as backup to a PC based communications application (e.g., soft-phone) for their mission critical assured service (C2) voice communications needs if and when the PC or application fails.*

  Note: This is "not a finding" in the event the PC, PC communications application, and the network to which it is attached can be proven to provide the reliability and availability needed to support assured service communications. This would be approximately equal to that achieved using an ASLAN and purpose built hardware based endpoints.

  Note: Applicability of this requirement can vary based on the specific use case and situation. For example, this is "not applicable" in the event a C2 user is in a situation where there is no need to place or receive priority calls. In a remote connectivity use case, a DoD provided PED, private cell phone or regular phone could serve as backup.

Note: Voice communications is the most critical communications service for C2 users. While VTC and collaboration is an important C2 tool, a telephone call is the minimal method needed to give and receive orders. Since a PC based application may not be available at all times, backup voice communications methods are needed. This could be accomplished in several ways. Minimally, in the normal workspace, there needs to be a hardware based telephone, either IP or otherwise, connected to a different portion of the network than the PC. While a hardware based IP phone could be associated with the PC, if the portion of the network serving the PC was the cause of the PC being inoperable for C2 communications, the phone might also not be available or operational.

2.4 User Operation of the Communications Application and Accessories

Users of PC based voice, video, UC, and collaboration communications applications must operate the application and their accessories in a manner that protects non-communications session related information existing in the environment. The environment consists of the PC and the work area around it. Both contain information. The PC contains information in the form of files, open documents, and open windows not actively participating in a communications session. The work area contains several forms of information. The first form is the work area's contents and anything that is sitting on a desk, posted on a wall, or displayed on a workstation/VTC monitor. This is visual information that can be viewed by a camera such as a webcam that is placed in the work area. The second form of information found in the work area is audible information. This can consist of non-communications session related telephone conversations or conversations between co-workers. Some of this information could be sensitive or even classified.

Another concern is the potential for communications session information including aural or visual content, being disclosed to individuals in the area of the PC, which are not part of the communications session. Users must be cognizant of who can overhear or see the contents of the communications particularly if the content is sensitive or classified. Such external persons might not have a need-to-know the information they see or hear, and may not hold the proper security clearance for the information. Communications endpoints that participate in classified communications may be required to adhere to certain limitations such as location, position, headset use, and so forth, to mitigate these concerns.

These concerns apply to all communications sessions whether they are supported by hardware endpoints such as speakerphones or VTC units, or PC based software communications applications. Mitigating these concerns consists of implementing various policies and procedures along with user training in the proper care, use, and protections required. User training must be augmented by a combination of user agreements and user guides. These mitigations will be discussed later.

2.4.1 Information In View of a Camera

Users of PC based communications applications that employ a camera must not inadvertently display information of a sensitive or classified nature that is not part of the communications session while the camera is active. This can happen if information in the form of charts, pictures, or maps are displayed on a wall within the viewing, or capture range of a camera. Any Pan, Tilt, and Zoom (PTZ) capabilities of the camera must be considered. One may consider visual information out of range, but it may be in range considering camera capabilities such as high definition, PTZ, and video enhancement possibilities for captured frames. Inadvertent display of classified information could also happen if the information is laying on a desk or table unprotected.

- *(RTS-VTC 1120.01: CAT I) The IAO will ensure a policy and procedure is in place and enforced that addresses the operation of video/collaboration communications related cameras (e.g., webcams or VTC cameras) regarding their ability to inadvertently capture and transmit sensitive or classified information such that:*
  - *Conference room and office users do not display sensitive or classified information on walls that are within the view of the camera(s).*
    Note: while covering such information mitigates disclosure when a camera is to be used, if the camera is activated unexpectedly or without taking action to cover the information prior to activating, the information can be compromised. Best practice is to not display it in view of the camera at all.
  - *Conference room and office users do not place sensitive or classified information on a table or desk within the view of the camera(s) without proper protection. (e.g., a proper cover)*
  - *Conference room and office users do not read or view sensitive or classified information at such an angle that the camera(s) could focus on it.*

  Note: Vulnerability awareness and operational training will be provided to users of video/collaboration communications related camera(s) regarding these requirements.

Note: This requirement is relevant no matter what the classification level of the session. In an IP environment the classification of PC communications is dependant upon the classification of the network to which the PC is attached, and the classification of the facility in which it is located. While classified communications can occur at the same level of classification as the network and facility, communications having a lower classification or no classification (e.g., unclassified or FOUO) may also occur in the same environment. As such, sensitive or classified information that is not part of the communications session might be improperly disclosed without proper controls in place.

2.4.2 Audio Pickup and Broadcast

Microphones embedded in or connected to a communications endpoint, PC, or PC monitor can be sensitive enough to pickup sound that is not related to a given communications session. They could pickup nearby conversations and other sounds. This capability could compromise sensitive or classified information that is not related to the communications in progress.

Speakers embedded in or connected to a communications endpoint or PC can be made loud enough to be heard across a room or in the next workspace (e.g., cube). This capability could compromise sensitive or classified information that is being communicated during a session.

Users must be aware of other conversations in the area and their sensitivity when using any communications endpoint, not only a PC based voice, video, or collaboration communications application. This awareness must then translate into protecting or eliminating these other conversations. A short range, reduced gain, or noise canceling microphone may be required. A push to talk microphone may also be required for classified areas. The microphone should be muted when the user is not speaking as both a mitigation for this issue, and for proper etiquette when participating in a conference. The muting function should be performed using a positively controlled disconnect, shorting switch, or mechanism instead of a software controlled mute function on the PC.

Users must be aware of other people in the area that could hear what is being communicated. This is particularly an issue if the communicated information is sensitive or classified since the parties overhearing the information may not have proper clearance or a need-to-know. To mitigate this issue, a headset or speakers should be used and at a volume that only the user can hear.

- *(RTS-VTC 1080.01: CAT II) The IAO will ensure a policy and procedure is in place and enforced that addresses the operation of hardware based voice and video communications devices and PC based voice, video, UC, and collaboration communications applications with regard to their audio pickup and broadcast capabilities in relation to the sensitivity of the information communicated. Operational policy and procedures are included in user training and guides.*

2.4.3 Visual Compromise of Session Displays

When communicating using a PC based voice, video, UC, or collaboration communications application, the user must protect the information displayed from being viewed by individuals that do not have a need-to-know for the information. This is of additional concern if the information is classified and the viewing party does not have proper clearance. This is also a vulnerability for hardware based communications endpoints that display visual information. The mitigation for this is to position the display such that it cannot be viewed by a passersby.

- *(RTS-PC 1040.00: CAT II) The IAO will ensure a policy and procedure is in place and enforced that addresses the positioning of video displays associated with communications devices and PC based voice, video, UC, and collaboration communications applications with regard to the sensitivity of the information displayed and the ability of individuals, not part of the communications session, to view the display. Operational policy and procedures must be included in user training and guides.*

2.4.4 PC Data and Presentation Sharing

Visual collaboration often requires the sharing or display of presentations, open documents, and white board information to one or more communicating endpoints. While the technology for doing this is different between hardware based endpoints and PC based application endpoints, the vulnerability is the same. In both cases, the displayed information typically resides on a PC.

While in presentation/sharing mode, care must be exercised so that the PC user does not inadvertently display and transmit information on their workstation that is not part of the communications session and not intended to be viewed by the other communicating parties. Users must be aware that anything they display on their PC monitor while presenting to a communications session may be displayed on the other communicating endpoints. This is particularly true when the PC video output is connected to a VTC CODEC since the information will be displayed on all of the conference monitors. This presentation/sharing feature could result in the disclosure of sensitive or classified information to individuals that do not have a validated need-to-know or have the proper clearance to view the information. Thus the presentation/sharing feature presents a vulnerability to other information displayed on the PC if the feature is misused. This is a problem when sharing (displaying) a PC desktop via any collaboration tool using any connection method.

There is little that can be done to mitigate this vulnerability other than to develop policy and procedures to present to collaborative communications sessions. All users that perform this function must have awareness of the issues and be trained in the proper operational procedures. Such procedures may require that there be no non-session related documents or windows open or minimized on the PC while presenting or sharing. An additional requirement may be that the user may not permit others in a session to remotely control their PC.

- *(RTS-VTC 2440.01: CAT II) The IAO will ensure a policy and procedure is in place and enforced that addresses the proper implementation and use of the "Presentation and Sharing" features of collaboration applications and devices. This policy and SOP will be based on the specific application's or device's capabilities and will address mitigations for the possible inadvertent disclosure of information to conferees that have no need to see or have access to. Operational policy and procedures must be included in user training and guides.*

A similar issue is that some PC based collaboration applications can permit a user to allow other session participants to remotely control their PC. Depending upon how this feature is implemented and limited, it could lead to undesired activities on the part of the person in control and possible compromise of information that is external to the collaboration session. This would be the case if such sharing or remote control provided access to the local hard drive and non session related applications or network drives accessible from the controlled PC.

- *(RTS-PC 2450.00: CAT II) The IAO will ensure PC based collaboration application sharing and remote control features or capabilities do not provide unrestricted access to other (i.e., non shared) applications, the local hard drive(s), or other drives accessible through the network. i.e., the collaboration application will not provide, or will be configured to not provide, full remote control of the host (i.e., shared) PC. Sharing capabilities will be limited to the collaboration application and other applications or documents (e.g., document based applications and documents launched by the host PC user) specifically shared by the host PC user.*
- *(RTS-PC 2460.00: CAT II) The IAO will ensure PC based collaboration applications identify all connected parties whether on a two party call or in a multiparty conference.*
- *(RTS-PC 2470.00: CAT II) The IAO will ensure users of PC based collaboration applications are trained to only share control of their PC or applications with other users that they are familiar with and/or can identify as trustworthy.*

2.4.5 Audio and Video Capture When Not Communicating

The VTC STIG discusses the possibility of undesired or improper viewing of and/or listening to activities and conversations in the vicinity of a hardware based VTC endpoint, whether it is a conference room system or an office based executive or desktop system. If this was to occur, there could be inadvertent disclosure of sensitive or classified information to individuals without the proper clearance or need-to-know. This vulnerability could occur if the endpoint was set to automatically answer a voice, VTC, or collaboration call with audio and video capabilities enabled, or if the endpoint was compromised and remotely controlled. The stated requirements and mitigations involve muting the microphone(s) and disabling or covering the camera(s).

These or similar vulnerabilities could exist in PC based communications/collaboration applications due to an auto answer feature or compromised application or platform. As such, the simplest mitigation would be to only operate the software that accesses the microphone and camera when they are needed for communication. This does not work well for a unified communications application that is used to enhance our communications/collaboration capabilities since the application would be running most, if not all of the time when the PC is operating. In this case, the microphone could be muted and camera disabled in software as a mitigation. However, this also may not work well due to the possibility of the communications/collaboration application, microphone, or camera could be remotely activated if the platform or a communications application is compromised. In this case positive physical controls may be required. We must also rely on our defense in depth strategy for protecting our PC applications, including our communications applications, from compromise.

Physical disablement such as unplugging from the PC, using a physical mute switch, or covering a camera could work if using external devices. However, this mitigation would not work for embedded microphones and cameras as is the trend in laptops and monitors today. While it may not be easily feasible to physically disable an embedded microphone, the lens of an embedded camera can be covered.

- *(RTS-PC 1080.00: CAT II) The IAO will ensure audio and video pickup/capture capabilities of microphones and cameras associated with a PC are disabled or inhibited when not required for communications such that inadvertent disclosure of aural or visual information is prevented. Operational policy and procedures are included in user training and guides.*

Note: This requirement minimally involves muting the PC microphone and camera. If necessary, the camera lens must be covered, or the camera aimed at a blank wall to “mute” it. Ideally, the microphone and camera would be external devices and not embedded in the PC or an external monitor that could be disconnected from the PC when not needed. The external microphone and camera could remain connected to the PC if there was a positive physical disconnect or mute (shorting) switch for the microphone, and if the camera is disconnected by the switch or the camera lens is covered.

- *(RTS-PC 1085.00: CAT II) The IAO will ensure auto-answer capabilities of any voice, video, VTC, UC, or collaboration applications are disabled in the event the application provides audio or video communications services such that the microphone and/or camera could be activated automatically when an incoming call is received.*

  Note: This does not apply to text based communications such as IM that does not activate a microphone or camera.

2.4.6 Use of Soft-Phone Accessories

While a headset, microphone, webcam, combination headset/microphone, and even a combination webcam/microphone can be considered to be soft-phone accessories, these are also accessories for other collaboration and communications applications. These have been discussed previously and are not included in the topic of this section. Our discussion here relates to, soft-phone specific accessories, which consist of USB phones, USB ATAs, and PPGs.

A USB phone is a physical USB connected telephone instrument that associates itself with the soft-phone application running on the PC. It minimally provides a handset which includes both the mouthpiece and receiver and may provide a dial pad, a speakerphone function, or other functions. In general these devices do not pose a security threat other than those discussed previously under audio pickup/broadcast section above. They should be operated accordingly.

A USB ATA is a USB connected device that associates itself with the soft-phone application and provides the ability to utilize a standard analog telephone or speakerphone. Some USB ATAs also provide a port to which an analog phone line can be connected. This allows a single analog phone to be used with the soft-phone while also answering and placing calls via the analog phone line. This line could be connected to a local PBX or to the PSTN. Some USB phones contain a port to which an analog phone line can be connected so the USB phone can be used with it to place and receive calls. There is little risk in the operation of this kind of USB ATA or USB phone providing it operates only as described and there is no direct bridging of networks as described next.

A PPG (USB connected or internal card) is a type of ATA that is a gateway intended to bridge the soft-phone application and supporting VoIP network to an analog phone line from a local PBX or the PSTN. PPGs pose legal and fraud threats to a DoD network due to this bridging of networks. They can be used for toll fraud, toll avoidance, or placing or receiving unauthorized calls. Some USB Phones can contain a PPG. While these devices might be used to meet a specific mission requirement, their use may be illegal in certain countries and instances when connected between a DoD IP voice and data network and a public dial-up voice network.

The use of any soft-phone accessory that provides a network bridging function poses both a legal and an IA threat to the DoD voice communications network. PPGs must not be used except to fulfill a validated and approved mission requirement.

- *(RTS-PC 1121.00: CAT III) The IAO will ensure soft-phone accessories (i.e., PPGs, ATAs, and/or USB phones) capabilities are reviewed and their functionality tested or validated prior to approval, providing them to users, and implementation.*
- *(RTS-PC 1125.00: CAT III) The IAO will ensure personnel are trained not to employ personally provided soft-phone accessories (i.e., PPGs, ATAs, and/or USB phones). This policy is to be acknowledged in user agreements and included in user training and user guides.*
- *(RTS-PC 1130.00: CAT I) The IAO will ensure soft-phone accessories (i.e., PPGs, ATAs, and/or USB phones) that provide a network bridging capability are not used on a DoD PC or network except to fulfill a validated and approved mission requirement.*
- *(RTS-PC 1140.00: CAT II) In the event a soft-phone accessory providing a network bridging capability is approved for use to fulfill a validated and approved mission requirement, the IAO will ensure personnel are properly trained in their implementation and proper use. This training is to be acknowledged in user agreements and included in user guides.*

2.5 User Awareness and Operational Training, User Agreements, and User guides

Users of PC based voice, video, UC, and collaboration communications applications must be aware of, and trained in, the various aspects of the application's safe and proper use. They must also be aware of the application or service vulnerabilities and the mitigations for them. This awareness is supported by a combination of user training in the use of the application and any associated accessories as well as its limitations and vulnerabilities. Training is subsequently acknowledged through the signing of user agreements and bolstered by the distribution and utilization of user guides.

- *(RTS-PC 1220.00: CAT II) The IAO will ensure training materials are developed and PC based voice, video, UC, and collaboration communications application users are trained in, and aware of, various aspects of the application's safe and proper use as well as the application or service vulnerabilities. Training will include all items contained in user agreements and user guides.*

2.5.1 Acceptable Use Policy – User Agreement

DoDI 8500.2 IA control PRRB-1 regarding "Security Rules of Behavior or Acceptable Use Policy" states "A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access."

This IA control requires the generation and use of a "user agreement" that contains site policy regarding acceptable use of various information system (IS) assets. Requiring the user to read and sign the user agreement before receiving their government furnished hardware and software, or before gaining access to an additional IS, add on application, or an additional privilege, provides the required acknowledgement.

The Secure Remote Computing STIG requires that a user agreement be used and signed for a user to be permitted to remotely access a DoD network or system. The Wireless STIG adds policy items to this user agreement regarding the use of wireless capabilities in conjunction with remote access. This STIG will be no different in that we, the DoD IA community, must define acceptable use requirements for the use of PC based voice, video, UC, and collaboration communications applications and accessories. While the first two STIGs mentioned require a user agreement prior to remote access privileges being granted, the user agreement should be signed when the user receives their government furnished hardware that covers all acceptable use policies. These policies are to include such things as acceptable web browsing, remote access, all wireless usage, as well as the usage of communications applications, soft-phone accessories, stick phones, personally configured VoIP, and IM clients. Minimally, the user agreement must be updated as privileges and certain applications are installed. User agreements must also be accompanied with user training and guides that reiterate the agreed to policies and provide additional information such as how to implement certain features and IA measures as required.

- *(RTS-PC 1260.00: CAT II) The IAO will ensure users agreements are developed in accordance with DoD policies that address the acceptable use of PC based voice, video, UC, collaboration communications applications and their accessories. Topics to be covered are, but are not limited to, the following:*
  - *Users are not permitted to install soft-phone agents, soft-VTUs, and/or IM clients that connect to or use a public VoIP or IM service for personal use (i.e., non-official business).*
  - *Users are not permitted to install private soft-phone agents that communicate with other private soft-phone agents or personal phone gateways (PPGs).*
  - *Users are not permitted to use a stick-phone associated with a commercial VoIP service or a personal VoIP system on a DoD system unless sanctioned and provided by a DoD component or organization.*
  - *Users are not permitted to use soft-phone accessories that can provide a bridge (if connected) between the DoD communications application or DoD network and another computer, phone network, or the PSTN.*
  - *Users are not permitted to use the DoD provided soft-phone and/or soft-VTU intended for remote access while working in their normal DoD workspace (i.e., in the office) without permission of the IAO and via a special or properly configured network connection or the LANs remote access architecture.*
  - *Cautions and notice of the unreliable nature of PC based voice, video, UC, and collaboration applications communications such that C2 users are aware of and acknowledge the non-assured service nature of this communications media.*
  - *Cautions and restrictions for the use of PC based voice, video, UC, and collaboration communications application's capabilities when used in an area where classified work or discussion occurs with emphasis on "webcam" and speakerphone usage.*

  Note: The site may modify these items in accordance with local site policy however these items must be addressed in a user agreement. The user agreement may be stand alone regarding acceptable use of PC based voice, video, UC, and collaboration communications applications and their accessories or may be included in a larger user agreement that addresses remote access and/or workstation usage.

Note: To the extent possible, PC protection and monitoring mechanisms (e.g., HBSS) should monitor compliance with these requirements.

Note: Requirements supporting the above user agreement items may be discussed later in this document. The list above may not include all items that need be in the requirement based on the other requirements discussed.

2.5.2 User Training and User's guides

User agreements must be accompanied with a combination of user training and user guides that will reiterate the agreed to policies and prohibitions. The training and guides should also provide additional information such as how to operate a system or device and implement certain features and IA measures as required.

A user guide would be extremely helpful in providing information to the user for the proper usage of PC based voice, video, UC, and collaboration communications applications and remote access implementations in general. An item that must not be forgotten in such a user guide is a discussion relating to the use of a PC based voice, video, UC, and collaboration communications applications for assured service C2 communications. Cautions and notice of the potential unreliable nature of these communications applications or methods must be included in user guides so that C2 users are aware, and reminded of, the non-assured service nature of these communications methods.

There are other topics that should be contained in a user guide serving this purpose. One such topic is the use of a "webcam" with hardware or software based VTU, particularly when used in a classified environment. Another user guide topic is the possible use of speakerphone capabilities when using a hard or soft EI in environments where classified discussion or work occurs.

- *(RTS-PC 1320.00: CAT III) The IAO will ensure a user guide is developed and distributed to users of PC based voice, video, UC, and collaboration communications applications that minimally provides the following information:*
  - *Reiterates the policies and restrictions agreed to when the user agreement was signed upon receiving the communications application.*
  - *Provides cautions and notice of the potential unreliable nature of PC communications applications so that C2 users are aware and reminded of the non-assured service nature of this communications media/method.*
  - *Provides instruction regarding the proper and safe use of webcams in general and more specifically when used in a classified environment or where classified work is performed and/or classified material/information is displayed or used.*
  - *Provides instruction regarding the proper and safe use of speakerphone capabilities in general and more specifically when using them in environments where classified discussion or work occurs.*
  - *Provides instruction regarding the proper and safe use of presentation, document, and desktop sharing.*

Note: this requirement supported by DoDI 8500.2 IA control PRRB-1 discussed above.

2.6 Use Case Implementations and Protecting Critical Voice Communications

In the general vulnerability discussion above, we discussed the use of VLANs, ACLs, and separate voice and data subnets to provide protection zones on the converged LAN to protect our critical IP based voice communications (telephone) system and traffic. We also noted that this practice is extended to VTC systems and associated traffic as well as network management traffic. The following subsections will address the use or implementation of various PC based voice, video, UC, and collaboration communications applications in various scenarios or use cases along with the maintenance of protection zones integrity.

In general, the use of PC soft-phones by users in their regular workspace should not be permitted unless the soft-phone is their primary voice communications instrument. This is because the implementation of PC soft-phones in the LAN provides challenges to protecting the hardware based VoIP communications system. Having the PC soft-phone as the user's primary instrument presents additional issues for C2, life safety, emergency communications, and the overall voice communications system, thereby, making this scenario less than desirable from an IA standpoint. If PC soft-phones are not the user's primary instrument, and if required to meet a validated mission requirement, they could be implemented and used in limited numbers. The most desirable and logical use case for PC soft-phones is in a remote access scenario, where the user is away from their normal work environment.

2.6.1 Strategic LAN Use Case

A strategic LAN supports a permanent base, camp, post, or station, that is the organization's home (i.e., sustaining base) where the organization's day to day business is conducted. A strategic LAN is different than a tactical LAN which is deployed away from the organization's sustaining base and is usually temporary in nature.

The unfortunate nature of PC OSs as well as voice, video, UC, and collaboration communications applications, is their use in the LAN works against the protections afforded by the protection zones provided for in the VTC and VoIP STIGs. This is because the PC must be connected to, or have access to, the data zone by default for its data traffic while traffic from soft-phone, UC, or soft-VTC communications applications must access the voice and VTC protection zones. This exposes these zones and the connected hardware based communications and control devices/systems to compromise from the data zone.

Due to these constraints, all communications traffic emanating from a PC based voice, video, UC, and collaboration communications application is commingled with data traffic and receives the same treatment as data on the LAN. It is also subject to the same vulnerabilities that data has on the LAN. This allows communications traffic in the data zone to be subject to possible compromise and reduced reliability or a possible denial of service. Users must be made aware that their communications quality, reliability, and availability may be degraded when using PC based communications applications. This degradation will affect mission critical and life safety related voice communications in the workplace.

There is little that can be done about this situation without special enhancements to our LAN access switches, PC Network Interface Cards (NICs), OSs, and applications such that they can support multiple VLANs and IP subnets at the PC. While it is not customary for multiple VLANs and IP subnets to be supported by the typical OS and NIC or even the typical access port on a LAN switch, these capabilities are in development. In fact, several NIC vendors currently have models and supporting drivers available that can support multiple VLANs and IP interfaces. Communications applications are lagging in the ability to make use of this capability; however, these capabilities are also in development and it is only a matter of time until the capability and its usage is commonplace.

When running both data and communications applications on a PC, and when the communications traffic that must access a voice or VTC protection zone is split at the PC, the PC becomes a potential bridge between the data zone and the communications zones on the network. This allows additional potential attack vectors to be presented to the protected communications systems and devices. To mitigate this vulnerability the communications application, OS, or additional software (middleware), while splitting the traffic must protect the communications zones from compromise by applications that do not require access to those zones. This can become very difficult for a UC application that provides communications and other services that need to access both the data and communications zones.

The following subsections will discuss, and provide requirements for, several optional strategic LAN use case scenarios. These are as follows:

- Unified communications applications.
- PC Soft-Phone as the primary voice communications endpoint. (i.e., The elimination of hardware based instruments in the work area)
- Limited numbers of soft-phones connected to the LAN inside the enclave (i.e., as a secondary voice communications endpoint)
    - Soft-phones associated with another enclave
    - Soft-phones associated with a local VoIP system
    - Soft-phones associated with a CTI system

2.6.1.1 Unified Communications Applications in the Strategic LAN

UC applications integrate many data communications and collaboration services such as email, IM, multi-platform presence, voice and video chat, click-to-dial, and desktop sharing with telephone, voicemail, and traditional VTC communications services. These services are integrated such that the features or services can be used in just about any combination imaginable. These services primarily operate on PCs connected to the data domain or zone (VLAN(s)) while requiring access to the VoIP system controllers and possibly its endpoints and other servers. Capabilities and the location of servers differ from vendor to vendor. If not careful, a UC implementation could quickly degrade or eliminate the protections afforded the VoIP infrastructure by its VoIP protection zone.

Note: Methods for permitting the necessary PC traffic to, from, and between the voice and data zones while protecting the voice zone will be discussed later in this document.

2.6.1.2 Soft-Phones as Primary Voice Instruments in the Strategic LAN

This section discusses the implementation of PC soft-phones or UC applications as the primary and only communications device in the user's workspace. While this degrades the protections afforded a hardware based system, the trend is to use more and more PC based communications applications due to their advanced features, collaborative benefits, and perceived reduced cost. This soft-phone use case results in the elimination of hardware based telephones on user's desks in the workplace. This can be seen as, or result in, trading down (from a hardware based system) with regard to availability, reliability, and quality of service since the data network is generally more susceptible to compromise from many sources inside and outside the local LAN making the soft-phones more exposed to attack. This also means that there will be no telephone available in the workspace if the PC is not powered on, or the application is not loaded, or the PC is not fully functional. While this is undesirable from an IA standpoint, a business case can be developed to support it.

Note: The recommended relationship between PC soft-phone/UC applications and hardware based endpoints in the normal work area is that the PC application should augment the functionality of, or be a backup to, the hardware based instrument in the user's workspace.

The implementation of PC soft-phones or UC applications in the user work space as their only endpoint has several ramifications that must be considered. The following is a list of some of these:

- The PC becomes a single point of failure for communications services provided to a user in their workspace. A widespread problem, which affects many PCs or the network infrastructure, may disable all communications for many users at one time. Users may not even have a means to report the failure without using an alternate communications system. A fast spreading worm or power outage could create such a situation. While some may argue that "users can call on their cell phones", service may not be available or their use may not be permitted in the facility. This translates into the following:
  - The loss of functionality and efficiency as in lost time due to the inability to communicate when the PC or soft-phone application is not running or functioning properly.
- The protections afforded hardware based endpoints by the use of the voice protection zone such as VoIP VLAN(s), and others are missing for soft-phones in a widespread use/implementation scenario and, depending on the implementation on the PC, may degrade the protections afforded hardware based endpoints. Such is the case for all software based communications endpoints since they are typically implemented on all PCs and therefore will be connected to the data VLANs. Assured service for voice traffic will be degraded from that obtained with hardware based instruments connected in the voice protection zone. This translates into the following:
  - Additional IA measures being required to protect the VoIP infrastructure (e.g., a firewall between the VoIP and data VLANs).

- The hardware based endpoint is not available for use in parallel with, or in place of, the PC. This can be a problem if the PC is having performance or operational issues, is turned off, or is unavailable. Accessing help desk services requiring logging onto the PC to use the voice services and work on a problem could be a real challenge. Rebooting the PC to clear a problem would disconnect the call to the helpdesk. Accessing voice mail or answering the phone while the PC is booting is made impossible reducing efficiency, particularly when the user starts their day. If the user has C2 responsibilities, the IP equivalent of MLPP cannot function properly if application or PC is unavailable. Precedence calls will not be received by the user but will be transferred to their designated alternate answering point.
- Emergency communications could be unavailable if the PC is not booted, the communications application is not running, or either is otherwise compromised. Voice communications must be readily available for life safety and medical reasons, as well as other facility security emergencies. A partial mitigation for this in a "soft-phone world" is to place common use hardware telephones within a short distance (e.g., 30 to 50 feet) of every workspace which is an additional cost. This additional distance however, could be an issue in a medical emergency where a worker might be alone in their workspace with their PC or voice communications application not functioning properly, they may not be able to reach the common use instrument depending upon the nature of the medical emergency. If the worker was suffering a heart attack or diabetic emergency, they could die. Business cases therefore need to include the cost of insurance and/or law suites for this eventuality.
- The previous 2 items translate into the following:
  - The addition of common use hardware based instruments placed around the facility (for backup and emergency usage) along with the additionally required LAN cabling and access switch ports.

While some may feel that this is not an IA issue, in reality it is since the discussion is truly about availability, which is one of the prime tenets of IA. Additionally, the VoIP controllers (i.e., the equipment that controls the telephone system) must be able to be accessed by the PC soft-phones while being protected as they would be in a normal VoIP system using hardware based instruments.

- *(RTS-PC 1520.00: CAT II) In the event PC soft-phones and/or UC applications are implemented as the primary telephone endpoint in the user's workspace, the IAO will ensure the VoIP controllers, gateways, and hardware based instruments are protected in a VoIP VLAN structure in accordance with the VoIP STIG.*

Note: Methods for permitting the necessary PC traffic to, from, and between the voice and data zones while protecting the voice zone will be discussed later in this document.

- *(RTS-PC 1530.00: CAT II) In the event PC soft-phones and/or UC applications are implemented as the primary telephone endpoint in the user's workspace, the IAO will ensure C2 and special C2 users are provided with hardware based telephone instruments (VoIP or otherwise) or an alternate C2 communications system, minimally as a backup for instances where the PC or soft-phone/UC application is nonfunctional.*

- *(RTS-PC 1540.00: CAT II) In the event PC soft-phones and/or UC applications are implemented as the primary telephone endpoint in the user's workspace, the IAO will ensure hardware based telephone instruments, are installed within a short distance (e.g., 30 to 50 feet) of every workspace to be used for backup and emergency communications.*

The Designated Approving Authority (DAA) responsible for the implementation of a telephone system which primarily uses PC software applications for its endpoints must be made aware of the risks of operating such as system as well as the benefits. This is because the DAA must personally accept the risk of operating the system. In addition, the commander of an organization whose mission depends upon such a telephone system must also be made aware and provide their approval.

- *(RTS-PC 1560.00: CAT II) In the event PC soft-phones and/or UC applications are implemented as the primary telephone endpoint in the user's workspace, the IAO will ensure the command structure as well as the DAA approves the implementation or transition in writing. Approval documentation will be maintained by the IAO for inspection by IA reviewers or auditors.*

2.6.1.3 Limited Numbers of Soft-Phones in the Strategic LAN

This use case addresses situations whereby the soft-phone/UC application and PC is not the primary voice communications "device" in the work area. This means that there is a validated mission need and the number of PC soft-phones permitted to operate inside the LAN will be less than the number of hardware based phones in the LAN. This number should be limited to those soft-phones required to meet specific mission requirements. UC applications that are ubiquitous in the LAN are addressed later, however, typically these work in association with a hardware based phone system, not in place of it.

There are three possible scenarios for the use of limited numbers of soft-phones in the strategic LAN. We will discuss the first two in this section and the third in the next section.

The first of these scenarios is providing support for soft-phones associated with a VoIP system in another enclave. This is a remote access scenario and must operate as they would in a normal telework/remote access use case. We will discuss this use case later, however, if this scenario is approved, special accommodations must be made in the local LAN to support users from a remote LAN and permit them to connect to their home enclave. This could include segregating them on a separate dedicated LAN with its own boundary protection or by implementing a dedicated VLAN protection zone while opening the enclave boundary to permit the remote connection.

Note: Approval for this scenario would also require approval for specific foreign (non-local) PC attachment to the local LAN. These topics are beyond the scope of this document.

The second of these scenarios is providing support for soft-phones associated with a local VoIP system. It is preferred that PC soft-phones associated with the local VoIP system not be used in the LAN, at all, due to the difficulties they present to the protection of the local hardware based VoIP infrastructure. Under normal circumstances, due to the separation of the VoIP and data VLANs a PC soft-phone application (associated with the local VoIP system) should not be able to register with the VoIP controller and function when the PC is connected to the LAN. This is because the PC connects to a LAN access port assigned to the data VLAN(s) and traffic between the voice and data VLANs is blocked. Similarly, if the PC was to be connected to a LAN access port assigned to the VoIP VLAN(s), the soft-phone might work but the PC would not have its normal data connectivity or services.

If PC soft-phones are to be used in the strategic LAN, except as noted in the section on discrete instrument replacement, their numbers should be limited to those that are essential to the mission and additional protections ,as discussed later in this section, must be added to the LAN to maintain the protection of the VoIP infrastructure.

Implementations of limited numbers of PC soft-phones along with the protections afforded them and the local VoIP infrastructure must be approved by the responsible DAA.

- *(RTS-PC 1620.00: CAT II) In the event that limited numbers of PC soft-phones are to be implemented in the strategic LAN, the IAO will ensure the responsible DAA approves their use along with the measures implemented to protect these soft-phones and the local VoIP and/or data infrastructure. Approval will be provided in writing and will be maintained by the IAO for inspection by IA reviewers or auditors.*

If limited numbers of PC soft-phones associated with the local VoIP system are to be implemented in the strategic LAN, a separate protection zone or VLAN structure must be implemented for them. The purpose of this VLAN is to provide a means whereby the PC can access the services it requires in both the data and VoIP VLANs while protecting the VoIP infrastructure and enhancing soft-phone reliability, performance, and security. Implementation of such a VLAN must not provide an access path as in a bridge, between the VoIP and data VLANs. Traffic must be filtered such that the soft-phone's VoIP traffic is routed to the VoIP VLAN while all other traffic is routed to the data VLAN. This should happen at only one location such as a core router or firewall, however, the PC might be capable of this itself.

Note: Limited numbers in this scenario means as few as possible but may mean 25 or 30 percent of the overall PCs on the LAN. Beyond this percentage, the protections afforded by this implementation become limited or negated because of the large number of PCs in the soft-phone VLAN.

Note: Methods for permitting the necessary PC traffic to, from, and between the voice and data zones while protecting the voice zone will be discussed next in this document.

2.6.1.4 Voice/VTC Infrastructure Protection RE: PC Communications Applications

As discussed earlier, The VoIP STIG requires the segregation of voice and data traffic on the LAN via the use of VLANs, ACLs, and separate voice and data IP address space, thereby creating a voice protection zone. This is needed to help protect the VoIP infrastructure from attack and helps its provided services survive problems occurring in the data side of the network. Also as discussed earlier, PC based communications applications that interact with the VoIP infrastructure degrade and can negate the protections afforded it by its protection zone. This section will discuss various methods for maintaining the viability of the voice protection zone when PC communications applications are used.

- *(RTS-PC 1720.00: CAT II) In the event a PC based communications application (e.g., PC soft-phone, soft-VTC, UC, or collaboration) is implemented for use in a LAN supporting a VoIP telephone system or hardware based IP VTC system, the IAO will ensure traffic between the required voice protection zone, VTC protection zone, and data zones (VLANs) is tightly controlled to allow only the traffic that is required to operate the application and its features without significantly degrading or eliminating the protective qualities of the voice or VTC protection zones.*

Note: the following options are recognized as viable options for meeting this requirement providing they are configured properly and are effective. Some may be conditional based upon the use case.

- Require all traffic from a PC connected to the LAN which includes all communications application traffic, to travel in the data zone. Traffic that is required to access the VoIP infrastructure in the voice protection zone must traverse a VoIP aware stateful inspection firewall between the VoIP VLANs and data VLANs that is operated in accordance with the VoIP STIG. This solution is for use cases where there are limited numbers implemented or the PC and application are the primary communications endpoint. The primary negative for this solution, besides cost, is that critical voice communications from the PC is not protected as it would be in the voice protection zone. As such it will be more subject to compromise and reduced quality or reliability.
- In the event limited numbers of PC based soft-phones are approved for use in the strategic LAN, a dedicated VLAN or protection zone can be implemented to support those PCs supporting the approved soft-phones. Traffic into and out of this VLAN/zone is controlled at an easily manageable location (e.g., a single location possibly at the network core) such that VoIP traffic is routed to the VoIP VLAN(s); all other traffic is routed to the data VLAN(s); and traffic is prevented from passing between the VoIP and data VLANs via this VLAN.

- Require the LAN access layer switch to which the PC is connected to route traffic to the appropriate VLAN. This requires that the switch be able to distinguish the traffic that needs to go to the VoIP VLANs while routing all other traffic to the data VLAN. This could work if the only PC communications application implemented is a voice soft-phone that is intended to be part of the VoIP phone system since there would be only one source of signaling and VoIP media. As we implement and use other PC based communications applications such as VTC, UC, and collaboration, the ability to distinguish becomes difficult since these use the same or similar protocols. Some traffic from these applications may travel in the voice zone instead of the data zone which could cause the application to not function properly. Applications may have to mark their packets such that they are routed appropriately.
- Require that the PC and communications application route the traffic to the appropriate voice, VTC, and data VLANs. To do this the following is required:
  - Option 1: The PC will be fitted with two NICs that can be connected to two ports on the LAN access switch(s); one port assigned to the voice zone (VLAN(s) and subnet) and the other to the data zone. Installing two NICs may be easy for a fixed PC but difficult for a portable PC such as a laptop. Two LAN cable drops are required for this implementation adding to the cost. A third NIC may also be needed if the PC supports a soft-VTC client.
  - Option 2: Alternately the PC will be fitted with a single 802.1Q VLAN capable NIC having appropriate drivers and OS support. This NIC will be configured to connect to both the voice zone (VLAN(s) and subnet) and the data zone using a single cable drop. In the event the PC supports a soft-VTC client, the NIC will be configured to access the VTC protection zone if implemented per the VTC STIG.
  - The communications application or additional software will be required to tag, address, control, and route traffic appropriately such that it enters the proper zone (VLAN). Traffic requiring access to the components in the voice protection zone or VTC protection zone will be routed there while all other traffic will be routed to the data zone. Traffic that is from a soft-phone or UC application that communicates directly with the VoIP system endpoints or session controller will be routed to the voice zone. Traffic that is from a soft-VTC application that communicates directly with hardware based VTC endpoints will be routed to the VTC zone. The data zone is the default zone for all traffic including voice and video traffic not associated with the VoIP phone system or hardware based VTC system. This traffic includes all traffic normally associated with PC applications such as client server applications, file transfers, email, IM, collaboration, web services, and so forth, as well as non telephone or VTC system voice and video traffic such as that associated with IM, Chat, and collaboration applications.
- Alternate solutions may be employed as they are developed providing they meet the overall intent of the requirement and can be validated as such.

2.6.1.5 PC Soft-Phones and CTI Systems

The third scenario in which limited numbers of PC soft-phones might be used in a strategic LAN is when they are associated with or are actually part of a Computer Telephony Integration (CTI) application. Traditional computer telephony integration CTI encompasses the control of a telephone or telecommunications switch by a computer application. Interfaces are developed to provide connection between the computer, typically a workstation, and the telephone or other terminal attached to the telephone switch, and possibly a special analog or TDM line going directly to the telephone switch. Applications are also developed to make use of these interfaces to integrate a data application with the telephone system. Sometimes the integration is as simple as being able to dial a number from the computer application or it could provide full control of the switch as in the case of an operator's console. In these traditional scenarios, the voice stayed in a traditional telephone set and the data stayed on the computer with the exception of the control information. If the voice does enter the computer, it is sent directly to the sound card or converted to a sound file for storage and possible file transfer. The voice communication is not transmitted in real time via IP protocols. In contrast, modern day CTI is changing in that today the voice communications and control is being transmitted using IP protocols and the hardware interfaces and telephones are being replaced by computer applications.

Note: the CTI systems discussed here are not unified communications applications although some of the features are similar. CTI systems generally have a special function and are not a general user application. CTI typically involves integration with a database application as would be the case in a call center or help desk operation.

In this scenario, where soft-phones are an integral part of the CTI system/application, implementation of separate voice and data zones could be detrimental to the proper functioning of the application. While separation requirements should be enforced if possible, they could be relaxed providing the general CTI requirement of treating the CTI system as an enclave is followed. A system such as this should have its own VoIP controller. If the system needs to communicate with systems outside the CTI system enclave, proper boundary protection must be provided. For example, since IP soft-phones are prevalent in today's call center / helpdesk systems, such a system would require the ability to place and receive phone calls from outside the CTI enclave. Calls might leave and enter the enclave via VoIP or a TDM media gateway. The workstations and call center agents may also need to email and access the web.

Note: we have established that a network supporting a CTI application must be segregated from the enclave general business LAN and that this can be accomplished by maintaining a closed network or a segregated and access controlled sub-enclave having appropriate boundary protection. This is in support of DoDI 8500.2 IA control DCSP-1 regarding "Security Design and Configuration / Security Support Structure Partitioning" which states "The security support structure maintains separate execution domains as in address spaces, for each executing process by means of partitions, domains, etc., including control of access to, and integrity of, hardware, software, and firmware that perform security functions."

- *(RTS-PC 1660.00: CAT II) In the event a CTI system/application (e.g., call center, helpdesk, operators console, E911 system, etc) utilizing or incorporating PC based soft-phones are approved for use in the strategic LAN, the IAO will ensure the following:*
  - *The supporting network is configured as a closed environment (enclave) or a segregated and access controlled sub-enclave having appropriate boundary protection between it and the local general business LAN or external WAN.*
  - *In the event the CTI application accesses resources outside this enclave and there is the potential of the application being compromised from external sources, the supporting network is configured to provide separate voice and data zones and maintains separation of voice and data traffic per the VoIP STIG if technically feasible (i.e., such separation does not break the CTI application or there is another compelling reason)*
  - *The supporting network enclave and boundary protection is configured in substantial compliance with the Enclave, Network Infrastructure, and VoIP STIGs.*
  - *The CTI application /enclave (e.g., a call center application) is supported by a dedicated VoIP controller.*

2.6.2 Tactical PC Soft-Phone Use Case

The tactical arena is an ever changing fast paced environment. Commanders and units alike rely on information that is delivered via tactical IP networks. These networks initially must be able to be deployed quickly with a minimal amount of equipment, manpower, and skill sets. Initial deployments may include as little as a half dozen workstations or as many as fifty. Once the initial deployment is in place, the network may grow and become relatively permanent as would be the case for a rear command or logistics center or the deployed network may move regularly.

Traditional voice communications has long been part of tactical deployments using small deployable TDM based telecom switches. These systems require the laying of an additional voice cable plant to that required for the data network. VoIP technologies are changing this to a degree. The cabling for a VoIP phone can be a separate cable as in traditional telephony; however, the VoIP cable is now part of the data network cable plant. The cable plant size can also be reduced by using one cable to serve a VoIP phone and a workstation at the same time providing the VoIP phone meets the VoIP STIG requirements for this situation. Other communications applications such as VTC, IM, and collaboration are also enabled by the IP based tactical network.

The convergence of tactical telecommunications systems with tactical data networking systems is causing the telecommunications and networking skill sets to be converged as well. As a result, the tactical unit can do more with fewer people. The convergence of these systems also means that those “fewer people” need to take less equipment with them when deploying, resulting in reduced transport costs due to the use of fewer and possibly smaller pallets.

The need, prevalent in the tactical telecommunications and networking community, to reduce the size of initially deployed systems or packages makes a strong case for the use of portable PC such as a laptop, based applications providing voice, video, UC, and collaboration capabilities. Unfortunately these applications, when used in a tactical environment, possess the same vulnerabilities as are discussed throughout this document for the strategic environment. Therefore the network supporting a tactical VoIP communications system should follow the same guidelines as a network supporting a strategic VoIP system or application. In the tactical environment, hardware based IP phones and the supporting voice protection zone will still provide more voice communications reliability if the data zone is compromised than if not used.

An argument could be made that a tactical LAN and attached workstations might be less prone to compromise than a strategic LAN and its attached workstations therefore we do not need all these security measures for VoIP. This argument could be supported by the smaller size of a tactical LAN, particularly an initially deployed system, mission duration, and the ability to limit its usage to tactical applications. Unfortunately if the tactical LAN is connected to NIPRNet or the strategic LAN at the home base, it can still be compromised particularly if general web browsing is permitted and performed and email is used. Additionally, there is nowhere that C2 communications is more important than in the tactical LAN. Any decision to eliminate any of the protective measures for the C2 voice service that could negatively impact its reliability must be based in a risk assessment that weighs the benefits against the risks.

Deployable packages that are designed to be initially deployed with a small footprint supporting or using PC soft-phones, which are then to be the basis of a larger network, must be configured, or be configurable, to support the separate VoIP and data zones as well as hardware based instruments and admission control for C2 communications as the deployed network and supported systems grow. The network will also include soft-phone protection zones as required in a strategic network if soft-phones are permitted to be used beyond the initial deployment. In general, larger relatively permanent tactical networks should be configured the same as a strategic network since similar vulnerabilities exist.

- *(RTS-PC 1820.00: CAT II) The IAO will ensure fixed tactical networks supporting IP based voice, video, UC, and/or collaboration communications are configured per the requirements for a strategic LAN.*
- *(RTS-PC 1860.00: CAT II) In the event IA configuration measures are reduced for highly mobile tactical networks (e.g., initial deployment packages) supporting hardware or PC based voice, video, UC, and/or collaboration communications, the IAO will ensure a benefit vs. risk analysis is performed, documented, and approved in the certification and accreditation of the system.*

Note: It is recognized that deployable packages for highly mobile tactical networks may only support PC based voice, video, UC, and/or collaboration communications applications. Such a network may not require separate zones for voice and data since all traffic will be in the data zone.

2.6.3 PED/PDA Soft-Phone Use Case

Personal Electronic Devices (PEDs) and Personal Digital Assistants (PDAs) are small form factor general purpose devices that operate on general purpose operating systems that support many different applications. Many of these devices also support wireless IP network and Internet access. As such these devices can, and sometimes do, support portable VoIP soft-phone applications that make use of wireless IP network access. Security requirements for PDAs and PEDs are addressed in detail in the Wireless STIG.

Any usage of a soft-phone on a PDA or PED must comply with the applicable soft-phone requirements detailed in this STIG and the platform must be configured and operated in compliance with the Wireless STIG.

- *(RTS-PC 1920.00: CAT II) The IAO will ensure a PED/PDA using IP wireless access and supporting a VoIP soft-phone is configured and operated in compliance with the wireless STIG. Additionally ensure the soft-phone application is configured and operated in accordance with the general communications application requirements in this STIG.*

2.6.4 Remote Access / Telework Use Case

While the use of many PC based voice, video, UC, and collaboration communications applications may be beneficial within and without the enclave, we have already established that it is better to use hardware based telephones instead of soft-phones for voice communications within the LAN or enclave. On the other hand, when outside of the enclave it is desirable and beneficial to have the ability to communicate using the VoIP system within the home enclave. When traveling it is impractical to take along a hardware based telephone along with the extra network equipment needed to connect it to the enclave's LAN. Thus, the most desirable and logical use case for the use of a soft-phone or UC application is in remote access situations. Other communications and collaboration applications are also used in this situation. Remote access is defined as the capability to access or use home enclave/LAN resources from a remote location outside the boundary of the home enclave. This location could be somewhere on the NIPRNet, a DoD component's Intranet, or more likely, on the Internet. Connections from "somewhere on the NIPRNet" or a DoD component's Intranet would be from within another NIPRNet connected enclave since we do not connect PC/ workstations directly to the NIPRNet. In such a case, connection of a "visiting" PC, not managed by the "other" enclave, to that enclave's LAN might not be permitted by local policy.

Note: This situation may be changed based on new remote access policy being developed by the DoD Chief Information Officer (CIO).

Therefore, the most likely remote access scenario will be from a location somewhere on the Internet while traveling or teleworking. Typically this will be from home, a telework facility, a contractor's facility, or a hotel, airport, etc. In some cases the access may involve wireless communications if permitted and enabled by the DoD organization providing the user with their PC/laptop.

DoDI 8500.2 IA control EBRU-1 provides DoD IA policy for PC remote access to the enclave. This policy is intended to protect the enclave and the PC along with the applications it supports. General remote access requirements are discussed in the Enclave STIG while operational and architectural requirements are covered and defined in great detail in the Network Infrastructure, Secure Remote Computing, and Wireless STIGs. These all define an encrypted client-to-site (or host-to-gateway) Virtual Private Network (VPN) architecture authenticated using DoD PKI certificates on DoD Common Access Cards (CAC). The VPN is to terminate at the enclave boundary; on the firewall or outside the firewall in a De-Militarized Zone (DMZ) such that the tunneled traffic into the enclave can be inspected by the firewall and Intrusion Detection System (IDS). Additional requirements apply as defined in the applicable STIGs.

PC based voice, video, UC, collaboration, and unified communications applications operating in a remote access scenario require the use of the same required remote access VPN back to the DoD home enclave (or a second one in parallel); Thus allowing the application to properly function and to be properly protected from various threats living outside the home enclave on other networks. These other networks are considered un-trusted in relation to the home enclave. Once a communications application accesses the home enclave LAN, it can function and be protected as if it were located inside the LAN.

- *(RTS-PC 2120.00: CAT II) The IAO will ensure PC based voice, video, UC, collaboration and/or unified communications applications operated in a remote access scenario utilizes an encrypted, properly authenticated, client-to-site VPN architecture that is in compliance with the following STIGs:*
  - *Enclave STIG*
  - *Network Infrastructure STIG*
  - *Secure Remote Computing STIG*
  - *Wireless STIG*
  - *Desktop Application STIG*

  Note: This requirement is not intended to determine the level of compliance with the applicable STIG(s). This is only a finding in the event that applicable STIG(s) have not been implemented.

  Note: this includes but is not limited to the following:
  - *The remote host computer connects to the "home LAN" through an encrypted client-to-site VPN connection.*
  - *The VPN is terminated at the enclave boundary (on or outside the firewall) such that the tunneled traffic can be inspected by the firewall and Intrusion Detection System (IDS).*
  - *Establishment of the VPN is DoD CAC/PKI authenticated.*

In addition to complying with the STIGs and VPN requirements noted in the previous bullet, there is an additional requirement for PC soft-phone and UC applications using the VPN. That is that soft-phone and UC application traffic which must interact or communicate with systems and devices in the voice VLAN/protection zone must be routed to that zone while the other data and communications traffic is routed to the data zone. This is to be accomplished without degrading the separation of these two zones, or bridging them together. This can be accomplished in a number of ways depending upon the LAN and its boundary/VPN architecture.

- *(RTS-PC 2220.00: CAT II) The IAO will ensure traffic from a PC based voice (i.e., soft-phone) or unified communications application, operated in a remote access scenario and using an encrypted VPN as required, is routed to the VoIP VLAN such that the separation of the voice and data zones is not degraded while all other traffic is routed to the data zone.*

2.7 Call Privacy and Confidentiality

When VoIP connections are established, call privacy may be significantly reduced when compared to traditional telephony. This is due to the ease of access to the call data from anywhere on the network. This is not only a problem on the LAN but more so across the WAN. To ensure the same privacy that subscribers expect, such as that provided by the existing PSTN and DSN, encryption must be implemented for all WAN connected calls. This can be accomplished in a number of ways. The best of these is end-to-end encryption, which in turn requires the IP telephone end devices to have greater processing power and the capacity to support encryption. This is not always feasible, as not all VoIP vendors provide encryption capability from the subscriber terminal. Additionally, until VoIP encryption standards are agreed upon and implemented, one vendor's method may not interoperate with others. In lieu of this, however, encryption should be accomplished at the link-level through the incorporation of High Assurance Internet Protocol Interoperability Specification (HAIPIS) or VPN technology as applicable. Gateway devices are normally designed to handle heavier processing loads and may also be capable of providing link encryption. Either method would be transparent to the subscriber community.

- *(VoIP0300: CAT II) The IAO will ensure that all VoIP traffic that is sent over approved VoIP enclave-to-WAN connections via an IP WAN network (i.e., Internet, NIPRNet,) is encrypted, at a minimum, between enclaves across the WAN.*

Note: The inherent site-to-site encryption employed in classified networks, such as the SIPRNet, meets this requirement.

It is highly recommended that end-to-end encryption of the VoIP conversation is employed. Secure Communications Interoperability Protocol (SCIP) or a Federal Information Processing Standard (FIPS) 140-2 validated encryption and key management method would serve this purpose well.

Note: Future guidance will require that all VoIP traffic will be encrypted end-to-end using specific protocols and encryption methods such that multi-vendor interoperability and assured service capabilities are achieved. Additionally, specific QoS requirements will be defined.

2.8 Application Requirements

The security and integrity of a PC and the network to which it is attached is reliant upon the security and integrity of the PC OS and the software operated on it. If either of these is compromised, the information housed on, or processed by, the PC can become vulnerable to any number of threats posed by the compromise. On the other hand, the compromise may pose a threat to the other devices connected to the network, (e.g., other PCs and servers). Such is the environment that we have to deal with in our networked world today. Since threats can come from a wide range of sources, we defend our networked PCs and associated servers using a defense in depth approach.

Today's trend toward the convergence of our previously dedicated voice and VTC communications networks with our data communications networks and its supported collaboration services ultimately places these communications at risk of falling prey to the same or similar threats and vulnerabilities suffered by the data network. If the PC has an application that provides voice, video, UC, and collaboration communications services installed, the communications service and/or information communicated can be at risk of compromise. This risk can subsequently place the overall communications system, its servers, and other associated communications endpoints at similar risk.

One of the many parts of our defense in depth strategy to limit threats and vulnerabilities to our critical time sensitive communications is to ensure the integrity of the PC's applications that support them. The following subsections will define requirements needed toward this end.

2.8.1 Certification, Accreditation, and Testing

Along with the measures described later to ensure application integrity, it is important that communications applications be tested and subsequently certified and accredited for IA purposes. This includes the applications as well as any upgrades and/or patches.

DoDI 8500.2 IA control DCCT-1 under "Security Design and Configuration / Compliance Testing" states "A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment."

This IA control relates to all PC communications applications and the accessories that work in conjunction with them such as USB phones or audio adapters, USB ATAs/PPGs, cameras, etc.

Additionally the specific network implementation(s) in which these applications are used must be addressed along with any central communications service for which the applications act as clients.

The DoD certification and accreditation process in defined by DoDI 8510.01; Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007.

- *(RTS-PC 3220.00: CAT II) The IAO will ensure PC communications applications are certified and accredited under DIACAP in association with, or as part of, their supporting communications system or service.*

- *(RTS-PC 3240.00: CAT II) The IAO will ensure PC communications applications are tested and approved prior to implementation.*
- *(RTS-PC 3260.00: CAT II) The IAO will ensure upgrades and patches to communications systems supporting PC communications applications are tested and approved prior to implementation.*

2.8.1.1 DoDI 8100.3 Policy Compliance and DoD Approved Products List

DoDI 8100.3 provides policy for the DoD that requires the testing and certification of telecommunications systems for Interoperability and Information Assurance (IA) while establishing an Approved Products List (APL) for certified and accredited products. Under Applicability and Scope, it states "This Instruction applies to the hardware or software for sending and receiving voice, data, or video signals across a network that provides customer voice, data, or video equipment access to the DSN, DRSN or PSTN." Additional statements in this section expand this to most devices or systems that are associated with providing telecommunications service.

The purpose of this testing is twofold. One aspect is to determine if a vendor's product or system meets DoD functional requirements and that it can interoperate with established or existing DoD systems. The other aspect is to determine if the system can be configured to meet DoD IA requirements and operate at an acceptable level of risk. A product must be approved under both categories before listing on the APL.

DoD components are required to fulfill their communications needs by only purchasing APL listed products, providing one of the listed products meets their needs. This means the APL must be consulted prior to purchasing a system or product. If no listed product meets the organization's needs, they may sponsor a product for testing that does meet their needs.

Note: The APL as created by this instruction was originally called the DSN APL and covered dial-up telecommunications systems or products providing unclassified communications. It has been expanded to cover additional types of approved products and has been renamed to the Unified Capabilities APL by the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII). Additional categories have been implemented for DRSN (classified communications) related systems/products and for IPv6 capable products. The APL can be found at http://jitc.fhu.disa.mil/apl/index.html. This APL is referred to as the DoD APL or UC APL.

Tactical use cases or systems that do not provide access to the DSN, DRSN or PSTN which are private closed communications systems, may be accredited via the Information Support Plan (ISP) or Tailored Information Support Plan (TISP) process managed by the Office of the Secretary of Defense (OSD), Joint Staff J6I, and the Joint Interoperability Test Command (JITC) United States (US) Military Communications Electronics Board (USMCEB) Interoperability Test Panel (ITP).

This policy applies directly to any PC communications application that provides voice communications services to and/or from the DSN, DRSN/VoSIP, or PSTN. This will most often be a soft-phone or unified communications application (with any associated accessories) that is associated with or supported by a DoD telephone system. The application may, or may not, provide additional communications services such as video, collaboration, or other unified communications services. This policy is extensible to other types of PC communications applications whose primary purpose may be VTC, IM, or collaboration, if the application or service provides interoperability with the DSN, DRSN/VoSIP, or PSTN typically through a gateway, or uses these systems for transport.

- *(RTS-PC 3320.00: CAT II) The IAO will ensure PC communications applications providing voice, data, or video communications interoperability with the DSN, DRSN/VoSIP, or PSTN, along with any associated accessories (e.g., USB phones, cameras, and USB ATAs), are interoperability and IA tested and placed on the Approved Products List (APL) prior to purchase, per DoDI 8100.3.*

  NOTE 1: APL listing of soft-phone applications, and/or associated accessories, will be in association with, or part of, the listed VoIP telecommunications switch/system that supports the application. Other applications (VTC or collaboration) will be listed with their core service or system.

  NOTE 2: This is not a finding in the event a PC communications application implementation and/or supporting system is not associated with, interoperable with, or connected to DSN, DRSN/VoSIP, or PSTN and is never expected to be.

Note: The DRSN is a custom and proprietary non-VoIP telephone system. It interoperates, to a degree, with a Defense Information System Network (DISN) VoIP telephone system/service on the Secret Internet Protocol Router Network (SIPRNet). This VoIP service is called VoSIP (see acronym discussion in the next note). The discussion/requirement here applies to PC communications application associated with VoSIP that ultimately can interoperate with DRSN endpoints.

Note: NSA defines VoSIP as Voice over Secure IP or regular (un-encrypted or encrypted) VoIP over any secure or classified IP LAN (i.e., local C-LAN) or WAN (e.g., SIPRNet or JWICS). In general VoSIP employs encryption at Layer 1 / Layer 2 applied to links between un-encrypted classified enclaves. The use of the acronym VoSIP for the DISN service and for instantiations on DoD component's classified LANs leads to confusion between the service and the intentional meaning of the acronym. NSA defines a similar acronym; SVoIP, meaning Secure VoIP. This refers to end-to-end NSA type-1 encrypted VoIP media and possibly signaling streams that can traverse a network having a lower classification. This is similar in concept to the secure voice service provided by a STU or STE as well as SCIP based devices. SCIP works at Layer 7 (application layer) and can use Type 1 or Type 3 encryption. It is not IP specific since it was developed for traditional fixed and mobile transport methods. Type 3 encryption of VoIP signaling and media is not SCIP. Unfortunately the SVoIP acronym/term has also been corrupted by some organizations using it to refer to their implementation of VoIP on their classified LANs and the SIPRNet WAN.

2.8.2 Communications Application Origin

Another one of the measures in our defense in depth strategy to protect our PC based voice, video, UC, and collaboration applications is to ensure the application originates from a reputable source. The source of these applications can vary depending upon the type of application. To protect DoD interests, the source of the application depends on the criticality of the communications method.

2.8.2.1 Freeware and Shareware

One source of possible compromise of a communications application is the use of freeware or shareware applications. This issue is covered in DoDI 8500.2 IA control DCPD-1 regarding "Security Design and Configuration / Public Domain Software Controls" which states "Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government."

- *(RTS-PC 3460.00: CAT II) The IAO will ensure freeware or shareware PC voice, video, UC, or collaboration communications applications are not installed or used except as detailed in DoDI 8500.2 IA control DCPD-1.*

2.8.2.2 Reputable Source and Software Integrity

Communications applications that primarily provide voice communications such as a soft-phone need to be designed to properly interoperate directly with the hardware based voice (VoIP) communications system. These applications should be a standard product of the voice system vendor or a partner whose product is approved by this vendor. The voice system is the most critical of all of the communications systems discussed in this document.

Communications applications that primarily provide VTC like communications can come from several sources. Some soft-phone applications provide VTC and collaboration features and should be sourced from the voice system vendor as noted previously. Applications that primarily provide VTC features and need to interoperate directly with a hardware based VTC system should be sourced from the VTC system's vendor or a partner whose product is approved by this vendor. Communications applications that primarily provide collaboration services while also providing voice and video communications features must also be sourced from a major vendor in the business of providing collaboration systems or services.

Unified communications applications that provide multiple services such as IM, presence, voice, VTC, web conferencing, and so forth, may also be a product of the PC's operating system vendor such as Microsoft.

Application sourcing can also be dependant upon whether the application is to interoperate with a hardware based communications system located and operated within an enclave or whether it is a system operated by an interagency or inter-base program.

This requirement is based on the fact that DoD components are required to use software and applications that are supported by a vendor that can maintain the security and integrity of the software or application. The vendor must be able to provide patches, upgrades or both to mitigate newly discovered vulnerabilities found in their product in a timely manner.

- *(RTS-PC 3420.00: CAT II) The IAO will ensure PC voice, video, UC, and collaboration communications applications are obtained from an approved reputable source such that the integrity of the application along with its interoperability and security is assured and that can provide support for the application to resolve operational and IA issues for DoD implementations.*

  Note: The following are applicable sources:
  - *Soft-phone and/or UC applications providing voice telephone services source from the enclave's voice (VoIP) system vendor (or their approved partner).*
  - *Soft-VTC applications source from the enclave's or program's VTC system vendor (or their approved partner).*
  - *Collaboration applications source from the enclave's or program's Collaboration system/service vendor (or their approved partner).*
  - *The PC's operating system vendor (e.g., Microsoft) providing the application is approved to interoperate with the primary systems above.*
  - *An AIS program that has sourced the application from an appropriate source and provided the necessary testing, certification, and accreditation.*

Additionally, it is important that the application is not modified during its delivery and installation. This can be a problem if the application is obtained from a source other than directly from it's original developing vendor such as a third party download service. Any application that is not obtained from its original developing vendor could be modified to add some sort of malicious code that could affect the confidentiality, integrity, and availability of the communications supported by the application. Also malicious code could affect the platform on which the application is operated, the network to which the platform is attached, and the communications system with which the application operates. To mitigate this issue, it is highly recommended that vendors provide their applications in a digitally signed and hashed format such that the integrity of the application can be verified.

- *(RTS-PC 3440.00: CAT II) The IAO will ensure PC voice, video, UC, or collaboration communications applications, upgrades, and patches are digitally signed by the vendor and validated for integrity before installation.*

2.8.3 Vulnerability Management

Managing, mitigating, or eliminating newly discovered vulnerabilities in a communications application is just as important as managing and mitigating the vulnerabilities of the platform supporting the application. As such, PC communications applications must be patched or upgraded when a security related patch or upgrade is released by the vendor. While many vendors will release a patch to mitigate a vulnerability in an operating system or major application, other vendors will include the fix in a new version of the application. Multiple patches can also be rolled up into an upgrade. It is important to maintain the current patch and upgrade level of any communications applications installed on a PC. The purpose of this is to maintain the highest possible level of security for the application and the communications service(s) it provides.

- *(RTS-PC 3520.00: CAT II) The IAO will ensure PC voice, video, UC, and/or collaboration communications applications are maintained at the current/latest approved patch or version/upgrade level.*

2.8.4 Application IA Configuration Considerations

There are several IA considerations that must be addressed to ensure PC voice, video, UC, and collaboration communications applications are operated safely. The following subsections address this topic.

2.8.4.1 Administrative Privileges

PC voice, video, UC, and collaboration communications applications must not be operated in a manner that can compromise the platform if the application itself becomes compromised. One way to mitigate this possibility is to ensure that the application does not require administrative privileges to operate and that it is not operated with privileges that could be used to compromise the platform, other applications, or the network.

- *(RTS-PC 3540.00: CAT II) The IAO will ensure PC voice, video, UC, or collaboration communications applications do not require and/or are not configured to operate with administrative privileges.*

2.8.4.2 Downloaded Configuration Files

Many communications applications are fully configured locally on the platform, however, in some cases they rely on a configuration file downloaded from the system with which they are associated. This situation also applies to hardware based endpoints. The integrity of these files is critical to preventing compromise of the application or hardware endpoint. The best method for maintaining the integrity of these files is to require that they be encrypted and digitally signed. This can prevent man in the middle attacks where the configuration file can be modified in transit or the source of the file spoofed.

- *(RTS-PC 3560.00: CAT II) The IAO will ensure downloaded configuration files for PC voice, video, UC, or collaboration communications applications that require configurations be downloaded from the system with which they are associated, are encrypted and digitally signed. The digital signature will be validated before the endpoint uses the file.*

  Note: To satisfy the encryption requirement here, the file can be encrypted directly (preferred) or downloaded over an encrypted channel.

  Note: This finding can be reduced to a CAT III in the event the file cannot be encrypted but minimally is digitally signed and the signature is validated before the file is used.

2.8.4.3 Server or System Association

All voice, video, UC, or collaboration communications endpoints must be configured to only associate with approved DoD controllers, gateways, and/or servers. While this is the norm for hardware based endpoints in a LAN, it is even more important for PC application based endpoints. Such endpoints must not accept service from just any available system. Such a system could actually be in a different organization than the one the application belongs to, depending upon how the application seeks out its controller/server. Peer-to-peer, or direct PC application-to-application communications are based on knowing the other endpoint's IP address is not permitted. All communications applications must contact their designated session controller(s), gateway(s), or server(s) for authorization to operate.

Note: This is the general rule for all communications types with the exception of point-to-point VTC sessions between hardware based VTC CODECs.

An additional consideration is the reliability of a critical voice communications service and its continuity of operations. This is a prime concern for hardware based VoIP systems which are intended or are designed to provide assured service. Such critical systems must be supported by redundant controllers. If a soft-phone associated with such a system is to be reliable, it must be configured to interact with its primary controller(s) and at least one backup.

- *(RTS-PC 3580.00: CAT II) The IAO will ensure PC based voice, video, UC, or collaboration communications applications are configured such that they only contact and associate with their designated and approved DoD controllers, gateways, and/or servers and their approved backups.*

2.9 DoD Policy for Non-Official use of VoIP and IM - ECVI-1 and ECIM-1

Various DoD policies disallow general PC users from installing any non-approved application on their workstations or from attaching any non-approved or non-government furnished devices to them. Still other DoD policies require users of government furnished equipment (GFE) (i.e., DoD PCs/workstations) to limit their use to official business and not use them for personal business or other personal activities. Additionally, and more specific to this STIG, DoDI 8500.2 IA controls ECVI-1 and ECIM-1 disallow general PC users from installing VoIP and IM clients that are intended to access public services for non-official, personal, use. An exception is made for the eventuality that such installations may be approved and performed by a DoD component for official business purposes. The IA controls state the following:

- ECVI-1: “Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary.

  Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function.”

- ECIM-1: “Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary.

  Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function.”

Note: AIS in this case means Automated Information System and relates to an official program.

The vulnerability is that installation of VoIP and IM clients that associate themselves with, and connect to a public VoIP or IM service places the DoD system on which the client is installed at risk of, and provides an avenue for, its compromise and unauthorized access. Once compromised, the system could be used as a launching point for further compromise of the network or other DoD systems. Additionally, the use of these services also places the confidentiality of DoD information conveyed by them at risk. Such information could be sensitive or the collection of non-sensitive information over time could reveal sensitive information.

The mitigation of the vulnerabilities presented by these public services requires a two prong approach. The first is a technical approach, while the second is an administrative approach requiring user awareness, training, and agreements.

A technical approach defined by the IA controls stipulates that traffic to and from public IM and VoIP services is to be blocked at the enclave boundary. It would be best if this were to occur at the NIPRNet Internet Access Points (IAPs), thus preventing such traffic from using the DISN, however this is not happening at this time since such blockage might also block other required services and the IAPs are not fully capable of such blockage at this time. This traffic must also be blocked at any Internet Service Provider (ISP) connection(s) to the enclave.

Note: All ISP connections must be approved and operated under a waiver obtained from the Global Information Grid (GIG) waiver panel.

It is the responsibility of the enclave to provide the required blocking since their firewalls and proxies are where the capability resides. To implement the mitigation, one might think that blocking specific IP addresses would be effective. This is not correct, however, since many of the public services have many IP addresses and servers, while they change their IP addresses regularly as a method of enhancing availability. Some of the public services have classically used non standard IP ports for their communications. Blocking these ports can be an effective measure in meeting the IA controls. Unfortunately, some of the public services are changing to use standard ports to get around the fact that many organizations block the nonstandard ports at their firewalls. The services are migrating to the standard ports 80 and 443 for web services which are generally never blocked.

While the purpose of blocking these public services in the network is that this mitigation will prevent the application or service from functioning properly in the event one is installed. It is best to prevent the user from installing the client applications. This can be accomplished by limiting a user's privileges on their PC such that they cannot install new software. This is typically done on many DoD PCs, however, some users require that ability. Also, unfortunately, just like the trend toward using standard ports, some services may function without a specific client by just using a web browser. This will most likely be the trend for the future.

A seemingly more effective approach to blocking these public services or prevent their installation is to block them by their URL. This might be done at a proxy in the enclave boundary or on the PC itself by listing the URLs as un-trusted and setting the PC or proxy security or protection level such that un-trusted sites are blocked.

- *(RTS-PC 4020.00: CAT II) The IAO will ensure PC based public IM and/or IP telephony services and/or supporting applications are unable to be used in the enclave in support of DoDI 8500.2 IA controls ECVI-1 and ECIM-1.*

  Note: This requirement does not include IM and/or IP telephony services and/or supporting applications implemented by a DoD component and approved for use by the responsible DAA to fulfill a validated mission requirement. (e.g., DISA's enterprise wide collaboration tools).

  Note: Examples of services to be disabled are, but are not limited to, the following:
  - *Yahoo Messenger*
  - *America Online (AOL) Instant Messenger (AIM)*
  - *Microsoft Network (MSN) Messenger*

- *Skype*
- *Freshtel*
- *Vonage*

The second mitigation for this vulnerability is the administrative prevention of the installation of the applications in question by the PC user. This is generally handled by today's policies and STIG requirements that are used to secure DoD workstations which limit the privileges of the workstation user. Users that are not given administrator rights on their workstations cannot install such applications. On the other hand, some users are given these rights. To cover those workstations on which the user can install software, the above policy must be enforced, and must be augmented by user awareness, training, and user agreements.

The limitations of these IA controls are extensible to hardware devices that provide the same or similar functionality. Such a device is a stick phone because it contains a client application. Such devices are available for commercial VoIP services such as Vonage and Skype. Another device that can be included under these guidelines is a PPG that connects a soft-phone to a traditional phone line permitting the uncontrolled bridging of voice networks.

- *(RTS-PC 4040.00: CAT II) The IAO will ensure:*
  - *Users are made aware and trained that even if their permissions allow, they are not to download and install IM and/or soft-phone applications on their DoD PCs that use or connect to public IM and/or IP telephony services unless directed to do so by their DoD organization for the fulfillment of an official requirement.*
  - *Users are made aware and trained that, they are not to attempt to use a stick phone on their DoD PC that associates itself or connects to a public IM or IP telephony services unless directed to do so by their DoD organization for the fulfillment of an official requirement.*
  - *Users are made aware and trained that, they are not to attempt to use a PPG on their DoD PC that associates itself with an installed soft-phone unless directed to do so by their DoD organization for the fulfillment of an official requirement.*
  - *The limitations in this requirement are listed in a signed user agreement.*

Note: DAA approval and possibly DISN DAA approval is required in the event IM and/or soft-phone applications, or stick phones that associate with or connect to a public IM or IP telephony service are to be implemented by a DoD component.

2.10 DoD Ports, Protocols, and Services Management

DoDI 8550.1 Ports, Protocols, and Services Management (PPSM) is the DoD's policy on IP Ports, Protocols, and Services (PPS). It controls the PPS that are permitted or approved to cross DoD network boundaries. Standard well known and registered IP ports and associated protocols and services are assessed for vulnerabilities and threats to the entire Global Information Grid (GIG) which includes the DISN backbone networks. The results are published in a Vulnerability Assessment (VA) report. Each port and protocol is given a rating of green, yellow, orange, or red in association with each of the 16 defined boundary types. Green means the protocol is relatively secure and is approved to cross the associated boundary without restrictions. Yellow means the protocol has issues that can be mitigated and it can be used if the required mitigations are used as noted in the VA. Red means that the protocol issues cannot be mitigated, is not secure, or approved in fact is banned when crossing that boundary. Typically "red PPS" carry a two-year removal notice.

A new rating category is Orange which is basically the same as red except that the protocol is in use and cannot be removed from the network. It recognizes that the protocol exists on the network and is necessary but also mandates that new systems and applications must not be developed using this protocol whether it crosses a boundary or not. Some red and orange protocols have mitigations listed in their VA that must be used if the protocol is used during its remaining life. The information regarding the assessed ports and protocols and the defined boundaries is published in the PPS Assurance Categories Assignment List (CAL). This is updated every month or so. See the Enclave and Network Infrastructure STIGS, the 8550.1, and the latest PPS CAL for a more complete discussion of this DoD program and policy. The PPSM information is available on the IASE and DKO/DoD IA Portal web sites.

2.10.1 PPS Registration

A portion of the DoDI 8550.1 PPS policy requires registration of those PPS that cross any of the boundaries defined by the policy that are "visible to DoD-managed components". The following PPS registration requirement applies to PC communications client traffic that crosses the IP based Enclave boundary to the DISN WAN or another enclave.

- *(RTS-PC 4520.00: CAT II) The IAO will ensure all IP ports and protocols that cross the enclave boundary and/or any of the defined DoD boundaries used by a PC communications client for which he/she is responsible are registered in the DoD Ports and Protocols Database in accordance with DoDI 8550.1.*

This page left intentionally blank

APPENDIX A - DEFINITIONS

The following definitions provide some insight to terms used in this document and the communications industry. They also provide some insight into the roots and the complexity of today's PC based communications applications. Also included are definitions of various PC peripherals including those referred to as soft-phone accessories.

A.1 Real-Time Communications

Real-Time Communications: Time sensitive; transmission method independent; communications between two or more individuals or entities that will be degraded or rendered unintelligible if portions of the information conveyed is lost, delayed, or garbled during its conveyance between the sender and receiver.

On a packet switched network such as an IP based network, each transmitted packet must be received with minimal latency, packet loss, and jitter. Examples are unidirectional or bidirectional (possibly interactive) audio and/or video communications such as in a voice conversation, video feed, or video conference. Audio communications is more sensitive to latency, packet loss and jitter than video communications. Specifications for worldwide end-to-end packet loss, latency, and jitter can be found in the Unified Capabilities System Requirements document under development for the Office of Secretary of Defense (OSD) by the DSN PMO and Real Time Services Working Group (RTS WG).

A.2 Near-real-time communications

Near-real-time communications: Time sensitive communications between two or more individuals or entities that can survive small amounts of delay or loss resulting in an automatic packet re-transmission. Such communications may be interactive and text based. Examples are telemetry, short messaging, IM, and white boarding or desktop/application sharing during a video conference.

A.3 Non-real-time or "best effort" communications

Non-real-time communications: The type of communications that IP protocols and IP networks are designed to support. Such communications can survive somewhat significant delay, some packet loss, and automatic re-transmission. This form of communications is best suited to data communications where the information must get there, but it does not need to get there right now. This is also called "best effort" communications. Examples are file transfers and email.

Note: Most, if not all of the near-real-time examples noted above typically receive "best effort" treatment on the network and can survive because "best effort" is generally pretty quick. Delays in message delivery affect the user experience and can lengthen an interactive communications session.

A.4 Real Time Services (RTS)

Real Time Services (RTS): Inelastic Services that provide or enable real time communications. While real time communications and therefore RTS are generally independent of transmission method, RTS is typically inferred to mean services provided by an IP based network that facilitate real time communications. (e.g., VoIP.). A real-time service typically requires strict bounds on packet loss, delay, and jitter. It cannot tolerate throughput variations based on network load level. (Net-Centric Implementation Document (NCID) T300 Version 2.0).

A.5 Voice Communications

Voice communications: refers to interactive audible communication of the spoken word occurring in real-time between two or more individuals using some form of technology (system/service) (e.g., telephone system or two-way radio).

A.6 Video Communications

Video communications: refers to interactive visual communication occurring in real-time between two or more individuals using some form of technology (system/service) (e.g., Video Tele-Conferencing (VTC) system). Video communications most often accompanies voice communications and permits the communicating parties to see each other. Video communications as in a VTC system can also include the visual display or communication of pictures, drawings, or the written word in near real-time.

A.7 Text Based Communications

Text based communications: refers to interactive visual communication of the written word in near real-time. (e.g., Instant Messaging (IM) or “texting”)

A.8 Telephone or Phone

Telephone or Phone: Originally known as an endpoint for a dial-up or circuit switched voice communication system such as the Public Switched Telephone Network (PSTN). Today the term also means an endpoint for a packet switched Voice over Internet Protocol (IP) (VoIP) based voice communication system. This device converts sound into electrical signals for transmission on the telephone network and receives electrical signals from the network which are converted to sound. These signals may be analog or digital in nature. Various connection methods have been used over the long history of the telephone. Today's phones include a numeric **dial-pad** that is used to transmit numbers to the central switching center which facilitates making connections through the network. Typically a phone consists of three parts, the base or **desk-set** which includes the dial-pad, the **ringer**, and the **handset**. The handset consists of a **mouthpiece** (microphone) and an **earpiece** (earphone/speaker). The ringer is a device (originally an electrical bell) that is used to signal an incoming call. It is typically part of the desk-set. A phone is also called an **instrument**. This is short for a telephone company term; subscriber instrument. The overall telephone system is designed primarily to provide two-party communications.

A.9 Speakerphone

Speakerphone: A telephone that possesses an amplified speaker and a microphone that is separate from the handset. The speaker and microphone may be internal or external to the desk-set and may be combined or separate. Today these are integral with the desk-set. A speakerphone is used for hands free communication after the communications session is established.

A.10 Videophone

Videophone: A telephone instrument that possesses a video camera and a video display that enables the two parties having a telephone conversation to see each other. Typically a videophone has a handset and dial-pad, and can also operate as a speakerphone.

A.11 Soft-Phone

Soft-Phone: An optional PC based software application designed to imitate, and provide the functions of, a hardware based telephone while using VoIP technologies. The DoDI 8500.2 IA control ECVI-1 identifies these applications as "workstation IP telephony clients". Soft-phones have had a long history. These applications were initially part of the development of VoIP communications which was to be used as a means to have cheap long distance voice communications over the Internet. This was driven, at the time, by the high cost of long distance service provided by the phone companies via traditional means. Early soft-phones were rather primitive in looks and behavior. As VoIP technologies developed as a replacement for traditional telephone systems and hardware, feature rich hardware based VoIP telephones were developed, primarily for business use. These telephones were, in some cases, able to surpass the feature sets of traditional business telephones. To keep pace, vendors of these business systems developed soft-phones to imitate their hardware based VoIP counterparts, both functionally and graphically. Some soft-phones, particularly generic ones, are capable of peer-to-peer operation while others require interaction with a vendor's VoIP Local Session Controller (LSC). Peer-to-peer operation only requires the IP addresses of the endpoints to make a connection. A VoIP LSC is the system signaling and control server which implements the telephone dial plan and provides other features and functions.

A soft-phone typically has the following characteristics:

- Provides a Graphical User Interface (GUI) on the viewing screen of the PC. The GUI may be a simple window that just displays a dial-pad and a dialed number box; it may imitate a basic telephone instrument; or may look like the hardware based VoIP telephone instrument (i.e., VoIP hard phone) of a particular vendor's VoIP system with which it is associated. In many cases the representation of the phone on the PC screen looks very much like a physical phone provided by the same vendor, right down to shape and branding.
- Dialing is performed via mouse clicks in the GUI or from the keyboard. Access to telephone features is also provided through the GUI.
- Uses the PC's internal sound card or an external USB attached audio adapter and instrument.
- Uses speakers and a microphone internal to, attached to, the PC making the PC work like a speakerphone. Optionally a headset in place of the speakers; a headset/microphone combination; or a USB attached audio adapter as part of a hand-set or desk-set can be used.

While a soft-phone can be part of a CTI system as one of the telephony components, the soft-phone itself should not be considered CTI. It is the computerized version of a telephony device. If on the other hand, the soft-phone seeks out phone numbers on the computer display such that clicking on the number will activate the soft-phone and dial the number, this functionality (called "click-to-dial") could be possibly considered a form of CTI.

The term soft-phone can also be used when referring to an add-on application to enable a portable computing device such as a Personal Digital Assistant (PDA) or similar general purpose portable computing device to provide voice communications over an IP based network. This is different than the software that enables a PED to place and receive calls over a cellular telephone network, making it a "Cell Phone" or "Smart Phone. While this document touches on PEDs/PDAs briefly, these soft-phone applications, while similar, are not the specific focus of this document. For the purpose of this STIG, the term soft-phone normally infers the PC based application.

To further alleviate any confusion, a soft-phone is not the required software that controls or operates a dedicated platform such as a cell phone or other portable phone or radio. This would be the device's operating system.

A.12 Computer Telephony Integration (CTI)

Computer Telephony Integration (CTI): The integration of traditional computer functions, software, and platforms with a traditional telephone instrument or switching system; primarily for the purpose of controlling the traditional telephony device from the computer or augmenting the telephony functions with additional capabilities, but not by providing the voice communications capability itself. The classic form of CTI has been used for operator's consoles; emergency services answering stations; and call distribution or call center systems (typically integrated with a database system for data retrieval and/or entry); automatic attendants; and Interactive Voice Response (IVR) systems. As technology has advanced and more and more things (traditional systems and devices) are being computerized, the meaning of CTI is seemingly blurred. A distinction needs to be made between computerization and CTI. The term CTI should be used in the classic sense, referring to the integration or interfacing of traditional computer functions to those of communications systems and devices; not the computerized replacements for traditional communications items (e.g., a soft-phone as defined later).

A.13 Voice over IP (VoIP) vs Circuit Switched Voice

Voice over IP (VoIP): A collection of technical methods and protocols for the control and transmission of end-to-end voice communications (typically bidirectional) across an IP based packet switched network such as today's LANs and WANs.

By contrast traditional **circuit switched voice** communications networks use a combination of analog and/or non IP based digital signals and transmission methods on the line side of the switching center (to the instrument) and uses non IP based digital time division multiplexing (TDM) on the trunk side of the switching center (i.e., between switching centers). The digital signals are generally pulse code modulated (PCM) audio with some signaling information added. Line side digital transmission is typically used in Private Branch Exchange (PBX) based business telephone systems.

A.14 Voice over IP and/or Video over IP - Acronym Confusion

Voice over IP and/or Video over IP - Acronym Confusion: VoIP generally refers to Voice over IP which means IP based voice services. Such has been the case since VoIP's initial development and is generally what is found when doing research on the subject. Unfortunately the acronym could just as easily refer to Video over IP, particularly because many of the same protocols are used. This can lead to extreme acronym confusion. While there are several acronyms that refer to unidirectional video over IP (e.g., IPTV), video is generally coupled with voice services for communications and collaboration purposes. As such various commercial entities are using acronyms such as VVoIP, V2oIP, and V/VoIP. (Note: V^2oIP is a registered trademark of RADVision Ltd.) For the purpose of this document, we will use V/VoIP to mean the general combination of bidirectional voice and video communications (together) over IP. V/VoIP can be added to other services to create a collaboration application. On the other hand, as noted above, VTCoIP refers traditional to full service Video-Teleconferencing over IP. V/VoIP is a component of VTCoIP which also provides additional services for collaboration.

A.15 Tele-Conferencing or Audio Conferencing

Tele-Conferencing or Audio Conferencing: A feature of the telephone network that enables multiple parties or telephones (typically more than two) to participate in a single conversation. The system facility that enables this feature is called a **conferencing bridge** (or conference bridge).

A.16 Video Tele-Conferencing (VTC)

Video Tele-Conferencing (VTC): An outgrowth of, or the combination of, the videophone and tele-conferencing. VTC was developed for businesses to enable them to hold meetings between geographically disbursed groups of people. As such they are typically large systems. VTC system endpoints include a coder/decoder (CODEC), speakers, microphones, video cameras, video displays, and a wired or wireless (typically handheld) control system or device. The displays are typically large and are built into meeting rooms or sit on a movable cart. The combined pieces of a VTC endpoint are referred to as a Video Tele-Conferencing Unit (VTU) while VTC refers to the technology. These terms are sometimes used interchangeably. Additionally, a VTU can be a single physical unit or device integrating all of the pieces noted above.

VTC endpoints can communicate directly like a phone or multiple endpoints can conference using a Multipoint Control Unit (MCU). The MCU is the VTC system's conference bridge. Access to the MCU is typically handled by a H.323 gatekeeper. While, a MCU can be a high capacity stand-alone infrastructure device, MCUs are also integrated into CODECs permitting small numbers of endpoints (typically 4 to 6) to conference on an adhoc basis without the need for an infrastructure MCU.

VTC systems which include the ability to share presentations to all participants along with white boarding capabilities are one of the earliest forms of collaboration tools.

As VTC has become popular and more reliable, the devices or systems have become smaller for use by a single person. These systems can be a cart full of equipment that sits in the corner of an executive office (called an executive system) or a single device that sits on the desk of an average worker. These desktop devices are similar to a videophone in concept but typically do not have the classic dial-pad and handset. Traditional VTC systems communicate over circuit switched networks using multiple Integrated Services Digital Network (ISDN) lines while newer systems can utilize IP based packet switched networks. IP based VTC can be referred to as Video Tele-Conferencing over IP (VTCoIP).

A.17 Desktop VTC

Desktop VTC: A dedicated hardware based device (i.e., VTC endpoint) that sits on a desk. The size of the unit is determined by the size of the display screen and is typically the size of an average PC LCD display. Its camera, microphone, and speakers are typically an integral part of (i.e., embedded in) the unit. A desktop VTC unit or desktop VTU is very similar to a videophone, but typically does not have the handset and physical dial-pad that characterizes a videophone. The VTU is typically controlled using an Infra-Red (IR) based handheld remote control. Some Desktop VTUs can also serve as the PC's primary or secondary display. Some vendors confuse this definition by calling their PC based soft-VTC application "desktop-VTC". For the purpose of this and related STIGs, the term Desktop VTC refers to the dedicated hardware based devices.

A.18 Soft-VTC or Soft-VTU

Soft-VTC or Soft-VTU: An optional PC based software application designed to imitate and provide the functions of a hardware based VTU. These applications were initially developed by VTC equipment vendors to permit PCs to interoperate with their hardware based product line. The applications typically have the look and feel of the vendor's hardware based products and are primarily intended to provide VTC services. They are capable of operating peer-to-peer or with VTC infrastructure devices such as a centralized MCU and gatekeeper. Some older soft-VTC applications work with a PC interface card that can connect to ISDN lines.

A soft-VTC application typically has the following characteristics:

- Provides a GUI on the viewing screen of the PC that closely mimics the look and feel of the vendor's hardware based VTC products' interface.
- Uses the PC's internal sound card.
- Uses speakers and a microphone attached to the PC making the PC work like a speakerphone. Optionally a headset in place of the speakers or a headset/microphone combination is used.
- Uses a generic USB connected camera ("web-cam") or a more capable VTC quality camera available from the VTC application vendor. High definition cameras are becoming available.

A Soft-VTC application may also provide standard VTC collaboration services such as white boarding, presentation display, data file transfer, and/or application and desktop sharing.

A.19 Webcam

Webcam: This term means many different things to different people. The classic meaning refers to any camera whose real time or near real time images are available on, or accessible via the World Wide Web from a PC with a web browser. There are many such cameras accessible via the Internet and private networks. These cameras can be connected to the network through computers such as PCs or servers, or can be directly connected to a wired or wireless network. IP CCTV surveillance cameras typically fall into the directly connected category, but are typically implemented on private networks. Another, and possibly more popular, meaning for this term refers to the little camera with the USB cable that we attach to our PCs to enable various video capture capabilities for the PC. Newer portable PCs as well as LCD monitors optionally contain embedded webcams. The capabilities of this type of webcam are dependant upon the installed drivers and applications that use it. For the purpose of this document, when referring to a webcam, we will mean a camera connected to a PC (via whatever means) that gives the PC an eye on the world in its immediate vicinity.

A.20 IP Television (IPTV)

IP Television (IPTV): The transmission of television programming (audio and video components) over IP, used generally for entertainment or information distribution purposes. The service is generally unidirectional, but may be interactive for program selection and ordering. IPTV is popular among telephone companies as a means of competing with the traditional cable television companies. IPTV can also be used to distribute information on an enterprise level Cable TV (CATV) network. As such, LAN cabling can be used in place of a dedicated CATV cabling infrastructure. IPTV systems include a device called a “set top box” that is used to connect the LAN to the television and acts as the decider for the transmission. IPTV can also traverse a Metropolitan Area Network (MAN) or WAN.

A.21 IP Closed Circuit TV (IP CCTV)

IP Closed Circuit TV (IP CCTV): An IP based Closed Circuit Tele-Vision (CCTV) system or the use of IP networks to transmit video from a surveillance camera to its monitoring station; also called IP Surveillance. Security or surveillance cameras have long been the key component of the CCTV industry. IP CCTV provides the capability to use LAN cabling in place of a dedicated CCTV cabling infrastructure. Standard CCTV cabling has inherent distance limitations. Fiber optic cabling extends these distances but is also limited. Digitizing the video signals and transmitting them using an IP/packet based can eliminate these distance limitations. This technology also includes protocols for the conveyance of camera controls such as Pan, Tilt, and Zoom (PTZ) from the monitoring station to the camera. As such, IP CCTV can be used to provide video surveillance of far flung remote facilities across a WAN such as the Internet. Also see Webcam.

A.22 Instant Messaging (IM)

Instant Messaging: Originally a PC based application designed to provide interactive text based communications between two parties in near real time across an IP based network. Multi-party IM is called Chat. Very simple IM applications can work peer-to-peer, but the more capable and more popular versions work with a central server. An integral part of IM is the "buddy list", a list of contacts or friends with which to communicate. This amounts to a simple directory, which has evolved to include indicators showing whether someone in the list is logged onto the service and is available for communications. As IM has developed over the years, additional services have been added to the system and applications such as graphics or icon display, file transfers, and real-time, videophone like, voice and/or video communications. IM has primarily been used as a social communications media over the years but is now being used more and more by the business community as a collaboration tool.
PC based IM applications that provide voice capabilities utilize the sound capabilities of the PC including internal or external speakers and microphones or attached headsets. Those that provide video capabilities typically use a USB connected camera (e.g., webcam).

While classic IM is a PC based application, it is not limited to PCs. IM clients are also available for portable devices such as IP (web) enabled PEDs and cell phones. This is not to be confused with "texting" (i.e., Short Messaging Service (SMS)) on a standard cell phone (non-IP or web enabled). "Texting" uses the signaling channels of the cellular transmission protocols and cannot directly communicate with an IP based IM client without a cellular gateway.

A.23 Presence

Presence: Originally the feature of an IM "buddy list" (when working with a central server) that can display whether individual contacts in the list are on-line and available for communication. Today's presence systems can be used by multiple applications and list multiple communications services or channels on which the contact is logged in and available (e.g., IM, regular phone, mobile phone, email, VTC) and which he/she wishes to be used first. Various busy and communications preference indicators are also available. Presence services are typically linked to a directory service in cross service or multi application implementations. Also see unified communications.

A.24 "Web Based" Application

"Web Based" Application: An Internet or Intranet based application whose user interface is generated within a general purpose PC application called a web browser (or just browser) used for browsing "web" (i.e., world wide web) pages. A web browser interprets HTML, Java, Active-X, or other mobile code transferred across an IP network to display web pages served up by (or requested from) a web server. A web server that provides the services of a specific application (e.g., time recording, expense reporting) is called an application server. Application servers utilize the same coding languages and mobile code as web servers, but also may require that specific browser plug-ins be installed such as Adobe Flash Player.

A.25 Web Conferencing

Web Conferencing: A web based application that provides some or all of the features normally found in VTC systems or applications. The primary focus is the presentation and white-boarding features of VTC with the possible addition of desktop sharing. While desktop sharing normally permits other conference attendees to see what is being presented from one PC, control of the presenting PC can be given to one of the remote attendees as selected by the operator of that PC. Web conferencing can also include multiparty webcam video display and/or audio conferencing as optional services. Some applications also add IM to the mix of features supported. The application server is the point that connects all of the PC endpoints together for the session and can be thought of as the VTC MCU which provides the same service for traditional hardware based VTC endpoints.

A.26 Collaboration

Collaboration: A process where two or more people work together toward a common goal; typically an intellectual endeavor that is creative in nature; by sharing knowledge, learning and building consensus. (Wikipedia.org). Collaboration can occur one-on-one or amongst multiple people; or locally as in a face to face meeting where all participants are in the same room; or it can occur remotely via any of the various communications methods available (e.g., audio conferencing, VTC, web conferencing, IM, the phone, etc). The common goal could be a consensus or decision as a result of a meeting or other discussion; or the development of a document or other product. Collaboration supported by technology requires communication between the collaborating parties. Collaboration can occur in non real-time using communications technologies such as e-mail; however this is not very efficient. Efficient and effective collaboration requires the use of one or more near real-time (text communications and document display) and real-time (voice and video) communications methods. Collaborative communications can also include other near real-time and non-real-time communications methods such as file transfer (non-real-time), screen/desktop sharing (VTC like display of information), white boarding (interactive markup of displayed information, and application sharing for multiparty editing in near real-time.

Collaboration is also a DoD buzzword referring to Web Conferencing and IM with or without integrated video and/or audio capabilities (e.g., DISA's Network Centric Enterprise Services (NCES) Button One (e-collab) and Button Two (Defense Connect Online (DCO)) collaboration tools or services.)

A.27 Collaboration Tool

Collaboration tool: a technological entity (e.g., system, device, software application) that enables the various communications methods required for effective collaboration to occur.

A.28 Collaboration Application

Collaboration Application: An optional PC based software application that facilitates collaboration using a wide range of communications types. The term is rather broad and means different things to different people, depending on their point of view and background. Most are deployed as a set of integrated or semi-integrated applications called collaboration tool suites. Most collaboration tools that provide communications services have their roots in IM. As IM has matured from a tool for social communications into a feature rich and capability rich business communications tool, the name has become "collaboration tool". In addition, soft-phone and soft-VTC applications can also be considered collaboration tools. Each of these tool types have different origins and were developed on different paths. Capabilities from the various types have been added to each and now all generally provide similar capabilities. Collaboration tool suites typically include IM, presence, voice and/or video communication, presentation and white-boarding, desktop and application sharing, as well as other features. As such, as with VTC systems, multiparty virtual meetings can be held with these applications and an appropriate central server or conferencing device.

A.29 Unified Messaging

Unified Messaging is the integration of voicemail, email, and fax. Email messages, voicemail audio files and fax images are stored as objects in a single mailbox. In many cases the audio and image files are stored as an attachment to an email message. PC users can open and listen to voice messages while fax images and email messages can be viewed or printed. A user can access the same mailbox by telephone locally or remotely. In addition to listening to voicemail messages, email messages can read to the user via a text-to-speech conversion. Unified messaging is often a component of unified communications suites discussed next.

A.30 Unified Communications

Unified Communications (UC) is the integration of different real-time and near real-time communications and collaboration systems, devices, media and applications into a single environment which offers the user a simpler, more complete, more effective experience. (Wikipedia.org, 2008). This integration can include fixed and mobile voice, video, and data communications services; unified messaging (email, voicemail, and fax); instant messaging; desktop and advanced business applications; VoIP and traditional PBX integration; cross system presence; web conferencing, collaboration, and white boarding.

UC's presence capabilities typically exceed those provided by a typical IM system. Presence and availability information extends across multiple platforms, systems, and communications devices. This can provide for the redirection of a communications session request; voice, text or email message; to the device closest to the intended recipient or to the recipient's preferred device (e.g., PC, fixed or mobile phone, PDA, etc) at any given time.

UC capabilities typically include a feature called “click-to-dial” or “click-to-communicate” whereby a user can click on a persons name or number in a directory and, using UC’s presence capabilities, the system figures out the best communications method to initiate the session or call. “Click-to-dial” telephone system integration can also locate telephone numbers in documents and web pages turning them into hyperlinks such that clicking on the highlighted number will initiate a telephone call.

In addition to providing an integrated user interface and experience, UC has the benefit of reducing "human latency" in business processes by making it easier to locate and communicate with a person who is needed to resolve an issue, answer a question, etc. Communications can occur almost instantly instead of waiting for that person to respond to a email or voicemail.

A.31 USB Phone

USB Phone: A USB connected computer peripheral used to augment a soft-phone application. It provides a hardware based interface like a telephone with a mouthpiece, an earpiece, and usually a dial-pad. USB phones take various forms such as just a handset, a non-flip style cell phone, or a complete desk-set. It may include an LCD display. It is typically recognized by the PC as an external audio device (i.e., sound card) which frees the built in sound card for other functions.

Like a headset/microphone combination, a USB phone adds privacy to the telephone conversation since the conversation is not played through the speakers to the user’s surroundings like a speakerphone. Additionally such headsets and USB phones can eliminate echo problems that are sometimes experienced when using the platform’s speakers and microphone. (Note: echo problems can also be overcome by using a high quality soft-phone application or appliance.) USB phones come in various configurations with various capabilities. Some USB phones can function as a speakerphone; some have a headset jack for use with a cell/cordless phone headset/microphone combination; some have wireless headsets. The predominance of USB phones are soft-phone specific and are compatible with and/or are intended for use with a specific commercial Internet Telephony Service Provider (ITSP) such as Skype or Vonage. There are, however, third party USB phones that are software compatible with major VoIP system soft-phones such as those from Cisco, Avaya, Nortel and 3Com. Nortel’s UNISTIM soft-phone implementation requires the use of their USB audio kit which is a headset adapter. Some USB desk-set models also include the capability of being used as a regular analog phone.

A.32 Analog Telephone Adapter (ATA) or Telephone Adaptor (TA) and USB ATA

Analog Telephone Adapter (ATA) or Telephone Adaptor (TA): A device used to adapt one or more standard analog telephones to a VoIP based business telephone system or an ITSP service. ATA and TA are different terms used for the same thing. The device is a converter that connects an Ethernet network (carrying the VoIP service) to a normal analog telephone via one or more Foreign eXchange Subscriber (FXS) ports. An ATA can also contain one or more Foreign eXchange Office (FXO) ports. A FXO port can be connected to an analog phone line (e.g., from the PSTN or DSN) that facilitates the placing and answering of traditional telephone system calls using the same analog phone.

USB ATA: A USB ATA is somewhat similar to a USB phone but has the express purpose of allowing a soft-phone to be answered and controlled by a standard analog telephone (to include cordless models). As with Ethernet ATAs these devices may also possess a FXO port that that supports the placing and answering of traditional telephone system calls using the same analog phone.

For clarity, a FXS port is one on which dial-tone and system battery is provided from the telephone switch. It is the jack in the wall. On the other hand, a FXO port is the jack on the phone or other device that is connected to the FXS port through the "telephone mounting cord". The phone receives its power (system battery) and the dial-tone through this connection.

A.33 Personal Phone Gateway (PPG)

Personal Phone Gateway (PPG): PPGs are also known as Personal VoIP Gateways. A form of ATA, usually a USB ATA, that has FXO ports instead of FXS ports. It provides the capability, and has the express purpose, of bridging the IP based voice network to a traditional voice network such as the PSTN via a PC soft-phone. The PPG and its associated soft-phone can then be used to place and receive calls to and from the local PSTN or PBX using another soft-phone on a remote PC located anywhere in the world. A PPG is typically installed at a PC located in a Local Access and Transport Area (LATA) (e.g., area code or country) where a user would like to place and receive local calls. The purpose of this scenario is to make free long distance phone calls to standard phones across the Internet, thereby bypassing normal long distance carrier toll charges. Conversely a call can be placed to a PSTN number and then via the PPG and soft-phone be carried across the IP network to another soft-phone. This soft-phone might have another PPG installed. PPGs also come in the form of a PCI card for internal installation in a PC. Some PPGs are sold in association with or as supporting Skype, an ITSP.

A.34 Stick Phone / Flash Phone

Stick Phone / Flash Phone: A specialized USB device that is intended to turn any PC into a VoIP telephone. It is based on a USB flash drive (sometimes called a thumb drive or memory stick after Sony's camera memory product) with an added audio adaptor and headset jack for use with a cell/cordless phone headset/microphone combination. The flash memory portion of the device contains an executable soft-phone application that is run on the PC. Some of these devices have onboard speakers and microphones while others support additional features such as doubling as a regular flash drive or MP3 player. While most are set up to associate with and connect through a particular ITSP (e.g., Vonage, Freshtel, or Skype), some are generic and will function with other services such as Google Talk and MSN. The primary purpose of these devices is to allow customers of an ITSP or similar service to make calls from any Internet connected PC such as those found in Internet cafes.

The term “Flash Phone” has also come to refer to a soft-phone like application.\ embedded in a web page that is based on Adobe Flash / Macromedia technology. This permits phone calls to be placed from within any web site by clicking on a “widget” on the page. The widget is the embedded soft-phone downloaded as mobile code with the web page. Usability assumes that the PC accessing the site has a compatible Adobe Flash enabled browser with a microphone and speakers. While this functionality can be provided using several different methods, the vendors or developers of the Adobe Flash based widget have dubbed their widget a Flash Phone. (Note: a full featured soft-phone, soft-VTC. And/or collaboration tool can be developed using Adobe Flash. An example of this is Adobe Connect, which uses Adobe Flash to provide a full featured VTC like collaboration tool. Such applications would not be considered as a “flash phone”.)

A.35 Internet Telephony Service Provider

Internet Telephony Service Provider (ITSP): A commercial service provider of IP based telephony service; sometimes called an IP Telephony (IPT) or VoIP service provider. ITSPs generally provide IP based PSTN subscriber line services to customers of broadband Internet Service Providers (ISPs). Service is typically delivered via an ATA to a traditional analog telephone. This service is intended as a replacement for the traditional analog line even though broadband service may be delivered over the same cable pair. ITSPs generally come in two types as follows:

- ISP based:
  - Traditional telephony service providers (i.e., Local Exchange Carriers (LECs) or Incumbent Local Exchange Carriers (ILECs) (e.g., Verizon, Quest, AT&T, etc) and potentially Competitive Local Exchange Carriers (CLECs) (e.g., Cavalier Telephone, Excel Telecommunications, US LEC, etc)
  - Cable television providers (e.g., Comcast, COX, Time Warner, Cablevision, etc.)
  - Other local and national ISPs
- Non ISP based third party providers (e.g., Vonage, net2phone, bbtelsys, PanTerra Networks, Freshtel, etc.)

In contrast, there are PC based VoIP services (e.g., Skype, Google Talk, MSN, etc.) that also use broadband ISP services pug can only loosely fit the definition of an ITSP. These are marketed in various ways but are generally advertised as free pc-to-pc (peer-to-peer) VoIP calling services across the Internet. Internet only sessions or “calls” between clients of the same or an interoperable service are the free part. Many of these services are based on an IM/presence application/service with an added dial-pad. Some may also provide voice and video communications capabilities as do most of today’s popular IM services. Some of these services (e.g., Skype, Freshtel, Yahoo Voice (formerly DialPad), etc) provide the ability to dial and call regular PSTN or mobile phone numbers (e.g., Skype-Out service) or to receive calls to an assigned phone number (e.g., Skype-In service) using a gateway to the PSTN. A fee is generally charged for these services. Some clients such as Skype’s implement a click-to-dial feature which also identifies the country in which the number is located.

A.36 Strategic LAN

Strategic LAN: A Local Area Network (LAN), Campus Area Network (CAN), or Base Area Network (BAN) that supports a permanent base, camp, post, or station. These sites are the sustaining base or home of any organization where the organization's day to day business is conducted. A strategic LAN/CAN/BAN is a permanent installation.

A.37 Tactical LAN

Tactical LAN: A LAN that supports a deployed tactical military unit; is generally small and mobile; is typically a temporary installation, and is designed to support a small contingent. As such, it may be less robust and less protected than a strategic LAN. A tactical LAN can grow to support a large number of endpoints, however as the tactical position becomes a permanent base of operations in a theatre; the LAN supporting it should transition from a temporary tactical design to a more permanent, more robust, more protected strategic design.

This page left intentionally blank

APPENDIX B - CNSSI 5000/5001 DISCUSSION

The Committee on National Security Systems (CNSS) (Formerly the National Security Telecommunications and Information Systems Security Committee (NSTISSC)) provides various forms of policy and guidance for the security and operation of national security systems (NSS) that store, process, and/or transmit national security information (NSI).

National Information Assurance (IA) Glossary, (CNSS Instruction (CNSSI) No. 4009) provides the following definitions for NSI and NSS and sensitive information:

- **National Security Information:** Information that has been determined, pursuant to (NSI) Executive Order 12958 (as amended) (Ref b.) or any predecessor order, to require protection against unauthorized disclosure.
- **National Security System**: Any information system (including any telecommunications system) used or operated by an agency or by a contractor of any agency, or other organization on behalf of an agency, the function, operation, or use of which:
  I. Involves intelligence activities;
  II. Involves cryptologic activities related to national security;
  III. Involves command and control of military forces;
  IV. Involves equipment that is an integral part of a weapon or weapon system; or
  V. Subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
  (B). Does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (Title 44 U.S. Code Section 3542, Federal Information Security Management Act of 2002.)
- **Sensitive Information**: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Based on the definitions noted above, NSI and NSS refer to classified information; and systems processing, storing, and/or transmitting classified information; respectively.

The National Telecommunications Security (NTS) Working Group (WG), formerly known as the Telecommunications Security Group (TSG) (author of TSG Standards 1 through 8), is the primary technical and policy resource in the U.S. Intelligence Community (IC) for all aspects of the Technical Surveillance Countermeasures (TSCM) Program involving telephone systems located in areas where sensitive government (i.e., classified information) information is discussed. TSG Standards will be replaced by and issued as CNSS Instructions (CNSSIs).

Director Central Intelligence Directive (DCID) No. 6/9, requires TSG Standards and Information Series compliance by Sensitive Compartmented Information Facilities (SCIFs) for the protection of sensitive information and unclassified telecommunications information processing systems and equipment; SCIF compliance shall now be fulfilled in accordance with the appropriate CNSSIs.

CNSSI No. 5000 supersedes NTSWG Standard 2b entitled "NTSWG Guidelines for Voice Over Internet Protocol (VoIP) Computer Telephony, dated April 2006" This document compliments the TSG standard 2 and NTSWG Standard 2a documents which addressed "Guidelines for Computerized Telephone Systems". CNSSI No. 5001 compliments the "Type-Acceptance Program" requirements documents; TSG Standards 3 and 4.

CNSSI No. 5000, entitled "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony," contains guidance for providing on-hook security for telephone systems located in areas where sensitive government information is discussed. The requirements established in this standard are necessary in order to achieve on-hook as an idle state, audio security for VoIP telephones and/or systems located in sensitive discussion areas. Implementation of this instruction does not preclude the application of more stringent requirements and may not satisfy the requirements of other security programs such as TEMPEST, COMSEC (Communications Security), or OPSEC (Operational Security).

CNSSI No. 5001, entitled "Type-Acceptance Program for Voice over Internet Protocol (VoIP) Telephones," specifies the design, construction, connectivity criteria, acceptance procedures, manufacturer's testing requirements, and documentation for VoIP type-accepted telephones. The requirements established in this instruction are intended to ensure that compliant devices cannot pass any audio via VoIP telephones and/or systems located in sensitive discussion areas when they are in an idle state (i.e., not in an active call).

The scope section of CNSSI 5001 states: "The provisions of this instruction apply to all VoIP Telephony Systems that currently reside, or will reside, in U.S. Government or U.S. Government sponsored contractor spaces where NSS are employed and/or within environments where classified NSI is stored, processed, transmitted, or when used as a point of isolation in accordance with reference b. (Telephone Security Group (TSG) Standard 2, "TSG Guidelines for Computerized Telephone Systems," Revised September 1993.)" The scope section of CNSSI 5000 is the same except for minor wording changes, the most significant of which is the addition of the word "unclassified" in the opening sentence between "all" and "VoIP". Since CNSSI 5001 was published after CNSSI 5000, we will assume the scope of both documents applies to both classified and unclassified VoIP systems.

Furthermore CNSSI 5000 and 5001 both mention "sensitive government information" and "sensitive discussion areas" While classified information is a form of "sensitive government information" (CNSSI) No. 4009 defines "sensitive information" specifically as unclassified information. Additionally, based on the definition of NSS, any telephone system, classified or unclassified, owned and /or operated by, or for, a DoD component, qualifies as a NSS since it can and most likely will "Involve command and control of military forces".

TSG Standard 1 on the other hand states that it applies to telephones located in government (or government contractor) sensitive discussion areas. It is concerned with on-hook audio security and does not apply to the interception of telephone conversations (Communications Security (COMSEC)). TSG 1 states that it is only valid for telephones located in physically protected spaces (PPS) and provides the following definition: Physically Protected Space (PPS): The space inside one physically protected perimeter. Separated spaces of equal protection may be considered to be part of the same PPS if the communications links between them are provided sufficient physical protection.

As such, the on-hook audio security requirements specified in CNSSI 5000 and 5001 seem to apply to all VoIP telephone systems whether classified or unclassified or whether the endpoints are located in classified or unclassified discussion areas.

As noted earlier, best practice dictates the implementation of all communications systems with endpoints that are designed to meet on-hook audio security requirements, whether the environment is unclassified or classified. Doing so will limit or eliminate the ability for an endpoint to allow aural information to be improperly disclosed through a design flaw or its compromise. Unfortunately, (as of March 08) there are no VoIP telephones that meet the CNSS 5000 requirements.

So, how does this discussion relate to the PCCC STIG? Surely if this STIG addressed DoD telephone systems or endpoints in general, whether traditional or IP based, all related TSG and NTSWG Standards as well as CNSS Instructions would apply, because these systems and their hardware based endpoints are the focus of these policies. These policies could spawn the inclusion of many requirements in the STIG related to on-hook or idle-state audio security. Minimally there could/would be a single requirement to use only TSG/NTSWG/CNSSI certified products in SCIFs and possibly other areas. Additionally, some of the requirements could also be extended to video security. Certainly endpoints capable of video communications should meet the audio security requirements along with minimally providing a positive, incontrovertible indicator that the video camera is active along with a positive method to mute or disable it.

As technology moves us away from using discrete hardware based communications endpoints to a single device having embedded microphones and cameras while supporting a software based audio and video communications environment, the ability to meet the requirements of CNSSI 5000 and 5001 for the telephony applications is lost unless significant modification of the supporting platform (i.e., PC) were to occur or external devices are required. As such, this situation could lead to a policy whereby a PC supporting a voice or voice/video communications application, and particularly those with embedded and cameras, are not permitted anywhere classified discussions could occur, or particularly in a SCIF. This is not the direction that DoD is headed since convergence everywhere is the plan.

The information in this section is provided to make the reader aware of issues that are not addressed by this document but possibly should be, and probably will be in the future. Before this can happen, the applicability of these requirements needs to be fully clarified. Interested parties may obtain copies of the CNSS instructions and other related documents by contacting the CNSS secretariat at 410.854.6805 or www.cnss.gov. U.S. Government contractors and vendors shall contact their appropriate government agency or Contracting Officer Representative regarding distribution of the CNSS documents.

This page left intentionally blank

APPENDIX C - ACRONYMS

ACL	Access Control List
AIS	Automated Information System
APL	Approved Products List
ASLAN	Assured Service LAN
ATA	Analog Telephone Adapter
BAN	Base Area Network
C2	Command and Control
CAL	Categories Assignment List
CAN	Campus Area Network
CATV	Cable TeleVision
CCTV	Closed Circuit TeleVision
CER	Customer Edge Router
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CLEC	Competitive Local Exchange Carrier
CODEC	coder/decoder
COMSEC	Communications Security
CNSS	Committee for National Security Systems
CNSSI	Committee for National Security Systems Instruction
DAA	Designated Approving Authority
DCID	Director Central Intelligence Directive
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DMZ	De-Militarized Zone
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoS	Denial of Service
DRSN	Defense RED Switched Network
DSN	Defense Switched Network
EI	end-instrument
EoIP	Everything over IP
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
FSO	Field Security Operations
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
GFE	Government Furnished Equipment
GUI	Graphical User Interface

GIG	Global Information Grid
HAIPIS	High Assurance Internet Protocol Interoperability Specification
IA	Information Assurance
IAO	Information Assurance Officer
IAP	Internet Access Point
IASE	Information Assurance Support Environment
IAVM	Information Assurance Vulnerability Management
IC	Intelligence Community
IDS	Intrusion Detection System
ILEC	Incumbent Local Exchange Carrier
IM	Instant Messaging
INFOCON	Information Operations Condition
IP CCTV	IP Closed Circuit TV
IP	Internet Protocol
IPT	Internet Protocol Telephony
IPTV	IP Television
IR	Infra-Red
IS	Information System
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ISP	Information Support Plan
ITP	Interoperability Test Panel
ITSP	Internet Telephony Service Provider
JITC	Joint Interoperability Test Command
JTF-GNO	Joint Task Force -Global Network Operations
LAN	Local Area Network
LATA	Local Access and Transport Area
LEC	Local Exchange Carrier
LSC	Local Session Controller
MAC	Mission Assurance Category
MAN	Metropolitan Area Network
MCU	Multipoint Control Unit
MLPP	Multi-Level Precedence and Preemption
MOS	Mean Opinion Score
NIC	Network Interface Card
NSA	National Security Agency
NCES	Network Centric Enterprise Services
NCID	Net-Centric Implementation Document
NII	Networks and Information Integration
NIPRNet	Non-Classified Internet Protocol Router Network

NTSWG	National Telecommunications Security Working Group
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSI	National Security Information
NSS	National Security Systems
OASD	Office of the Assistant Secretary of Defense
OSD	Office of Secretary of Defense
OPSEC	Operational Security
OS	Operating System
PBAS	Precedence-based Assured Service
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulated
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PPS	Ports, Protocols, and Services
PPSM	Ports, Protocols, and Services Management
PSTN	Public Switched Telephone Network
PTZ	Pan, Tilt, Zoom or Pan, Tilt, and Zoom
QoS	Quality of Service
RTS	Real Time Services
SCIP	Secure Communications Interoperability Protocol
SDN	Service Delivery Node
SIPRNet	Secret Internet Protocol Routed Network
SMS	Short Messaging Service
STIG	Security Technical Information Guide
STIGID	STIG Identifier
SVoIP	Secure Voice over IP
TA	Telephone Adaptor
TCP	Transport Control Protocol
TDM	Time Domain Multiplexing
T-ISP	Tailored Information Support Plan
TSG	Telecommunications Security Group
TSCM	Technical Surveillance Countermeasures
TEMPEST	Not an acronym, A discipline relating to signal emissions
UC	Unified Communications (also Unified Capabilities per ASD/NII)
UCAPL	Unified Capabilities Approved Products List
UPS	Uninterruptible Power Supply
US	United States
USB	Universal Serial Bus

USMCEB	Military Communications Electronics Board
UCR	Unified Capabilities Requirements
VA	Vulnerability Assessment
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VoIP	Voice over IP
VoSIP	Voice over Secure IP
VPN	Virtual Private Network
VTC	Video Tele-Conferencing
VTCoIP	Video Tele-Conferencing over IP
V2oIP	Voice and Video over IP – also V/VoIP or VVoIP
VTU	Video Tele-conferencing Unit
WAN	Wide Area Network
WG	Work(ing) Group

APPENDIX D - REFERENCES

Department of Defense Directive 8500.01E; Information Assurance (IA), Certified Current as of April 23, 2007

Department of Defense Instruction 8500.2; Information Assurance (IA) Implementation, February 6, 2003

Department of Defense Instruction 8510.01; Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007

Department of Defense Instruction 8100.3; Department of Defense DoD Voice Networks, 16 January 2003

Committee for National Security Systems Instruction (CNSSI) No. 5000; Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony, April 2007

Committee for National Security Systems Instruction (CNSSI) No. 5001; Type-Acceptance Program for Voice over Internet Protocol (VoIP) Telephones, December 2007

Committee for National Security Systems Instruction (CNSSI) No. 4009; National Information Assurance (IA) Glossary, Revised June 2006

Global Information Grid (GIG) Net-Centric Implementation Document (NCID) v2, Quality of Service (QoS) (T300): Signaling, Inelastic/RTS, Preferred Elastic and Elastic, 17 April 2006

IETF Internet Draft - draft-pierce-sipping-assured-service-02.txt
http://www.tools.ietf.org/html/draft-pierce-sipping-assured-service-02

Wikidedia.org, 1 May 2008, http://en.wikipedia.org/wiki/Mean_Opinion_Score